НАВЧАЛЬНО-МЕТОДИЧНА ЛІТЕРАТУРА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ
УНІВЕРСИТЕТ імені ІВАНА ПУЛЮЯ

КАФЕДРА ПРОГРАМНОЇ ІНЖЕНЕРІЇ

КОНСПЕКТ ЛЕКЦІЙ

з дисципліни

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

для студентів напряму підготовки
121 – інженерія програмного забезпечення

ТЕРНОПІЛЬ 2017

Конспект лекцій з дисципліни безпека програм та даних для студентів усіх форм навчання для напряму підготовки 121 – «Інженерія програмного забезпечення» /Упор.: Кінах Я.І. - Тернопіль: ТНТУ, 2017-52 с.

Конспект лекцій призначено для навчання студентів за напрямом підготовки 121 «Інженерія програмного забезпечення», та містить інформацію про структуру та зміст курсу безпека програм та даних.

Упорядник: к.т.н., доцент кафедри програмної інженерії Кінах Я.І.

Рецензенти: Р.П.Шевчук, к.т.н., доцент кафедри КН ТНЕУ,
І.З. Якименко к.т.н., доцент кафедри КІ ТНЕУ

Розглянуто на засіданні кафедри програмної інженерії, протокол № 1 від 31.08.2016р.

Лекція 1

Вступ до безпеки програм та даних

1. Основні поняття і визначення
2. Поняття криптографічної системи

1. Інформація – привселюдно оголошені чи опубліковані зведення про події і явища, що відбуваються в суспільстві, природному середовищі і т.д. (Закон України про інформацію).

Інформація - сукупність даних, програм і повідомлень, що обробляються чи зберігаються в системі, незалежно від фізичного чи логічного додатку.

2. Безпека інформації – захищеність даних, програм, повідомлень, протоколів, засобів, від порушення конфіденційності, цілісності, приступності і спостережності інформації.

3. Забезпечення безпеки інформації – сукупність заходів, спрямованих на забезпечення конфіденційності, цілісності, доступності і спостережності інформації. Основним засобом захисту інформації є застосування криптографічного перетворення.

4. Криптографічне перетворення інформації (КПІ) – перетворення інформації з метою забезпечення цілісності, підтвердження дійсності, авторства, захисту від несанкціонованого доступу, шифрування інформації, що здійснюється з використанням ключів.

5. Криптографічний захист інформації – захист інформації який здійснюється з використанням криптографічного перетворення.

6. Криптографічна система – сукупність засобів КЗІ, необхідної, ключової , керівної й іншої документації.

7.Засоби КЗІ – апаратний, програмний засіб, що призначений для КЗІ.

8. Ключові дані – сукупність випадкових чи псевдовипадкових значень змінюваних параметрів КПІ, за допомогою яких досягається мета КЗІ (забезпечується стійкість)

9.Послуги криптографічної системи – конфіденційність, цілісність, доступність і спостережність інформації і ресурсів в інформаційних системах і технологіях, що забезпечуються за рахунок застосування КЗІ.

10.Конфіденційність– властивість захищеності інформації від несанкціонованого доступу і спроб розкриття її змісту неавторизованими користувачами і (чи) процесами.

11. Цілісність – властивість інформації, що полягає в тім, що вона не може бути змінена випадково чи навмисно неавторизованими суб'єктами чи об'єктами.

12. Доступність – властивість ресурсу, інформації, об'єкта, послуги, системи, що полягає в тім, що об'єкт чи суб'єкт, наділений повноваженнями, може використовувати ресурс із заданою якістю, у тому числі за рахунок використання методів КЗІ.

13. Спостережність – властивість ресурсу, системи, що дозволяє реєструвати всі дії об'єктів і суб'єктів однозначно встановлювати імена об'єктів/суб'єктів, причетних до визначених дій, а також реагувати на всі дії з метою мінімізації втрат.

14. Криптографічний аналіз – аналіз криптографічної системи, її вхідних і вихідних параметрів, включаючи частину ключа з метою визначення значимої інформації, включаючи ключі, що можуть бути використані для порушення (11-13).

15. Інформаційна війна – протиборство непримиренних сторін в інформаційному середовищі, здійснюваної з метою нанесення максимальних збитків іншій стороні і мінімізації своїх збитків у різних сферах.

16. Інформаційна безпека – захищеність від впливів, природного чи штучного характеру в різних сферах.

17. Інформаційна зброя – сукупність організаційних і організаційно-технічних впливів на інформаційну чи систему інформаційну технологію, здійснюваних з метою розвідки, обміну і т.д.

Введення в криптографію

Найбільш загальною наукою про таємницю є криптологія. Криптологія як наука вивчає закономірності забезпечення конфіденційності, цілісності і т.д. критичної інформації в умовах інтенсивної протидії (криптоаналізу).

Криптологія поділяється на криптографію і криптоаналіз.

Криптографія - вивчає методи, алгоритми і засоби здійснення криптографічного захисту інформації.

Криптоаналіз – вивчає методи, алгоритми і засоби розкриття криптографічної системи при невідомій частині ключа.

Криптографічне перетворення інформації – здійснюється з використанням симетричних, несиметричних криптосистем. Криптографічна система називається симетричною, якщо ключ прямого перетворення збігається з ключем зворотного перетворення чи обчислюється один з іншого не вище чим з поліноміальною складністю (не більш 1 секунди).

Криптосистема (алгоритм) не симетричний, якщо ключ прямого перетворення не збігається з ключем зворотного перетворення, і один може бути обчислений з іншого не нижче чим з експоненціальною складністю.

$$\begin{cases} K_{пр.пр.} = K_{обр.пр} \\ K_{пр.пр.} \neq K_{обр.пр.} \end{cases}$$

У Європі криптопроект NESSIE –2000-2003, у ньому визначено 10 видів криптоперетворень

Симетричні – розробка блокового симетричного шифрування, потоковий шифр, автентифікація (процедура встановлення дійсності джерела, приймача повідомлень).

Несиметричні – функції хешування (обчислення криптографічних контрольних сум) односпрямованої хеш (стиску з великого простіра в малий), ключова хеш з використанням ключа.

Направлене шифрування (виконується умова (2)).

Ідентифікація (автентифікація) - (1),(2).

Криптопротокол - рішення розподіленої задачі, багатоетапно.

Лекція 2

Теоретичні основи забезпечення стійкості й автентичності

Структурна схема і математична модель системи КЗІ

1.Особливості забезпечення послуг конфіденційності, цілісності, дійсності, приступності, спостерігаемості.

2.Математична модель інформаційних об'єктів і суб'єктів.

Відповідно до прийнятого в захищених системах моделлю в інформаційному відношенні беруть участь 4 сторони: джерело й одержувач інформації, зловмисник (криптоаналітик), арбітр.

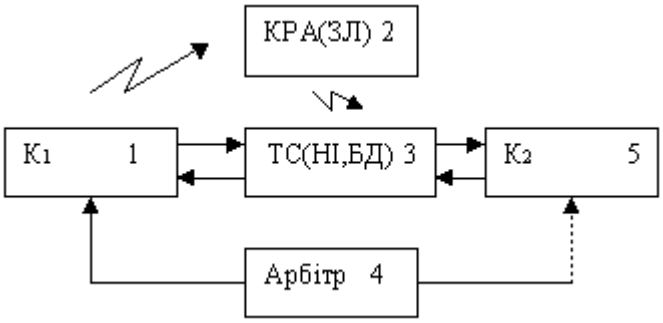


Рис.1.

У такій системі користувачі К1, К2 здійснюють інформаційні відносини і передається інформація з не захищеної телекомунікаційної системи, чи зберігається у відкритих базах даних, доступних носіях. У зв'язку з цим зловмисник має можливість здійснювати різного роду погрози з метою нанесення збитку К1, К2. Зловмисник буває:

1. Санкціонований користувач системи (порушник).
2. Криптоаналітик (КРА), зовнішній об'єкт – суб'єкт.

Порушник – фізична чи юридична особа, що навмисно (ненавмисно) здійснює в системі неправомірні дії, тобто з порушенням установленого порядку. Усі впливи на систему чи порушника КРА називаються погрози.

Погроза – потенційно існуюча небезпека впливу на систему з метою нанесення збитку системі, обумовлене процесом і обробкою інформації.

Погрози бувають активні і пасивні.

Пасивна – погроза, у результаті реалізації якої не змінюється інформаційний стан системи, але збиток наноситься.

Активна – зміна інформаційного стану системи.

Основні погрози, що може реалізувати КРА:

1. Компрометація захищеної інформації і ключів, у змісті одержання змістовної частини – розшифрування, ключі в явному виді.
2. Передачі через телекомунікаційну систему помилкових криптограм з метою обману К2.
3. Модифікація вірної інформації.
4. Порушення працездатності системи за рахунок передачі помилкових команд і сигналів.
5. Погрози, зв'язані з порушенням спостережності інформаційних відносин користувачів.
6. Несанкціонований доступ до інформації.

Для захисту від 1-6 погроз з метою забезпечення Д,С, Ц, П користувачі К1 і К2 повинні здійснювати КП. Як правило, з метою забезпечення Ц і П спочатку здійснюється цифровий підпис (ЦП) інформації Мі, формованої джерелом 1.

ЦП – функція КП.

$$ЦП = F_i^+(M_i, K_j, P_r) \quad (1)$$

Кj – ключ, Pr – доп. параметри, Мі – повідомлення, Fі – функція перетворення.

У результаті реалізації (1) повідомленню Мі додається цифрова сума (криптографічна контрольна сума, що обчислюється по (1).

Відображення простіру повідомлень $M_i^{'}$ безлічі криптограм Сі, процедура F прямого перетворення.

$$M_i^{'} \to C_i = F^{+}(M_i^{'}, K_j^{з}, P_r) \tag{2}$$

Криптограма Сі зберігається і передається відкрито.

Одержувач К2 чи К1 (якщо це носій інформації) при необхідності доступу до неї (M_i^{*}). П здійснює її розшифрування.

$$M_i^{*} = F^{-}(C_i^{*}, K_j^{P}, P_r) \tag{3}$$

Якщо в C_i^{*} немає помилок і використовуються узгоджено ключі і параметри, то M_i^{*} збігається з $M_i^{'}$, тобто з початком.

$$M_i^{*} = M_i^{'} \tag{4}$$

Для перевірки цілісності і дійсності інформації одержувач К2, використовуючи ключ перевірки цифрової області, перевіривши ЦП, обчислює зворотний підпис.

$$ОП = F_i^{-}(M_i^{*}, K_j^{'}, P_r) \tag{5}$$

Примітка:

a) К1, К2 повинні узгоджено використовувати ключі, у системі повинний бути джерело ключів, повинні бути система керування, ключ до даних.

b) Перетворення 1-5 повинні здійснюватися таким чином, щоб арбітр на їхній основі міг провести експеримент і винести рішення.

Математична модель

Більш докладно процеси перетворень розглянемо за структурною схемою (рис.2.2.)

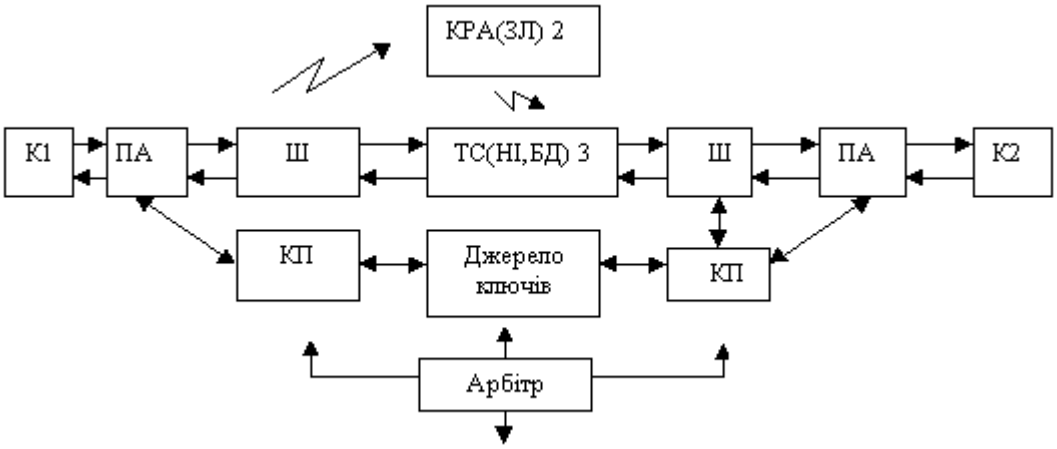


Рис.2.

Будемо вважати, що П1, П2 є джерелами повідомлень Мі для який відомі апріорний розподіл ймовірностей Р(Мі), $i = \overline{1, П_{сп}}$ і відома ентропія джерела повідомлень

$$H = -\sum_{i=1}^{П_{сп}} P(M_i) \log P(M_i) \tag{6}$$

Мі з метою забезпечення їх Ц, П автентифіцируються в пристрої 2 за законом ключа K_j^a . В результаті на виході формується M_i^a .

Шифратор 3 здійснює зашифрування за правилом (2), у результаті на виході шифратора формується виробництво криптограм Cj і будемо думати відомої апріорну статистику появи криптограм на виході шифратора - P(Cj).

Думаючи, що відомо імовірність:

$$P\left(C_j \middle/ M_i\right) = P\left(K_{ij}\right) \tag{7}$$

Фізичний зміст – за законом ключа Кj зашифрування.

Повідомлення Мі відображається в криптограму Cj і це дорівнює застосуванню Кij.

При передачі по телекомунікаційній системі на вхід шифратора 9 надходить C_j^*, *- факт можливості чи перекручування від перешкод, чи від КРА.

Розшифрування здійснюється за правилом (3), використовується Кj ключ расшифрования. У результаті на виході шифратора з'являється M_i^{a*} .

В ПА здійснюється обчислення відкритого підпису за законом ключа $K_j^{a'}$.

У результаті на виході 10 формується повідомлення M_i^* , цифровий підпис відрізається. Користувач одержує повідомлення.

Примітка:

Для працездатності системи П1, П2 повинні мати погоджені пари ключів, для автентифікації - ($K_J^a, K_j^{a'}$), для шифрування - ($K_j^з, K_j^p$). Ці функції виконує джерело ключів із ключовими пристроями.

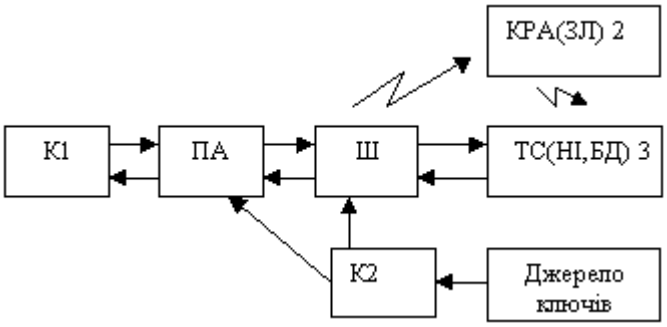
Якщо $K_j^a = K_j^{a'}$, система називається симетричної, якщо $K_j^a \neq K_j^{a'}$, система називається несиметричної.

Лекція 3

Безумовно стійкі КРС і їх реалізація

1. Математична модель КРС.
2. Умови реалізації БСС.
3. Відстань рівнозначності.

На рис. 3.1. приведена спрощена схема забезпечення криптографічного захисту повідомлень.



$$H(M) = -\sum_{i=1}^{n_m} P(M_i) \log_2 P(M_i) \qquad (1)$$

Рис.3.1.

Користувач К1 – джерело інформаційних повідомлень Мі, розмір джерела (кількість повідомлень) $i = \overline{1, n_M}$. Розмір ймовірність появлення повідомлення Р(Мі) апріорна ентропія Н(Мі) джерела інформації. З метою забезпечення цілісності і дійсності повідомлення Мі піддається криптоперетворенню – автентифікації, на виході формується Мі.

$$M_i^a = F_a^{-1}(M_i, K_j^a, P_r) \qquad (2)$$

Кj – ключ, обираний із простору ключів, розмірність $j = \overline{1, n_k}$.

Для забезпечення конфіденційності, M_i^a - повідомлення 2 піддається шифруванню, на виході формується Сj – криптограма.

$$C_j = F_ш^+(M_i^a, K_j, P_r) \qquad (3)$$

Сj передається К2 через ТС по відкритому каналі, чи записується на носій інформації.

КРА – зовнішня сторона, не входить у систему. Думаючи, що КРА знає Р(Мі) - апріорну статистику й ентропію Н(Мі), ставить задачу визначити яке повідомлення міститься в Сj і який ключ використовується для зашифрування Кj, і який ключ K_j^a використовується для автентифікації.

Думаючи, що КРА відомо апріорну статистику:

$$P\left(C_j \middle/ M_i\right), \qquad \forall i, j (i = \overline{1, П_м}, j = \overline{1, П_к})$$

Імовірність постановки задачі визначаємо імовірність того, що в Сj міститься Мj.

$P\left(M_i \middle/ C_j\right)$ - умовна апостеріорна імовірність.

КРА використовуючи $P\left(M_i/C_j\right)$ може знайти умовну ентропію $H\left(M/C\right)$.

$$0 \le H\left(M/C\right) \le H(M) \tag{4}$$

У процесі нагромадження криптограм КРА зменшує свою невизначеність, у результаті деяка інформація ΔI, яку можна вимірити:

$$\Delta I = H(M) - H\left(M/C\right) \tag{5}$$

Умовна імовірність $P\left(M_i/C_j\right)$ можна визначити використовуючи теорему:

$$P\left(M_i/C_j\right) = \frac{P(M_i)P\left(C_j/M_i\right)}{P(C_j)} \tag{6}$$

Реально, можна побудувати КС із 4 рівнями стійкості:

1. Безумовно стійкі КС чи теоретично не дешифруємі.
2. Обчислювально стійкі чи гарантован стійкі.
3. Ймовірно стійкі чи доказово стійкі.
4. Обчислювально не стійкі чи тимчасово стійкі.

Для класифікації можна використовувати різні показники і критерії. Найбільш кращим є використання наступних характеристик:

1) Nk – обсяг ключів.
2) H(k) – ентропія джерела ключів:

$$H(k) = -\sum_{k=1}^{n_k} P(K_i)\log P(K_i) \tag{7}$$

$P(K_i)$ - імовірність появи Кj – ключа в системі.

3) tб – безпечний час.
4) lo- відстань одиничності КС.

tб – математичне чекання часу розкриття КС із використанням конкретного методу. Найбільше простій – метод підбора чи грубої сили, тоді якщо потрібно перебрати N – варіантів, то

$$t_б = \frac{N_в}{\gamma K} P_T$$

P_T - імовірність, з яким необхідно здійснити криптоаналіз.

γ - продуктивність КАС, зміна кількості можливих переборів за секунду.

$K = 3{,}1 * 10^7$ сек/рік.

У граничному випадку Nв = Nк, де Nк – N ключів.

Т.3.1.

Необхідною і достатньою умовою теоретичної недешифруемості чи безумовної стійкості є умова:

$P\left(C_j/M_i\right) = P(C_j)$, тобто імовірність появи (8)

Криптограма в системі не повинна залежати від того, яке повідомлення обране. Фізично це означає, що будь-яке повідомлення може відбитися в будь-яку криптограму з рівною імовірністю.

$$P\left(C_j / M_i\right) = P(K_{ij}) \tag{9}$$

Доказ: визначимо імовірність $P\left(M_i / C_j\right)$, що може обчислити КРА .

$$P\left(M_i / C_j\right) = \frac{P(M_i) P\left(C_j / M_i\right)}{P(C_j)} \tag{10}$$

Якщо $P\left(M_i / C_j\right)$=P(Mi) – КРА не одержав ніякої інформації про Cj.

$$\frac{P(C_j / M_i)}{P(C_j)} = 1 \tag{11}$$

$P(C_j / M_i) = P(C_j)$ Відомо дві системи, що забезпечують безумовну стійкість: система Вернама і система «гаряча лінія».

Система Вернама

У системі здійснюється потокове шифрування, тобто символи криптограми в шифраторі шифруються за правилом:

$$C_i = (M_i + K_i) \tag{12}$$

Mi – i- тий символ, $i = \overline{1, n_M}$

Результат – символи ключа.

Відмінною рисою є те, що символи ключа Кі породжуються випадковою порівняно ймовірностною послідовністю, випадковим процесом. У такій системі в символів (довжина ключа) повинне бути не менш довжини повідомлення.

$$l_K \le l_M \tag{13}$$

$$M_i = (C_i - K_i) \bmod m \tag{14}$$

Сі – символи криптограми.

Кі – символи ключа.

m – підстава алфавіту.

Аналіз (12) і (14) показує, що для зашифрування і розшифрування потрібно використовувати ту саму випадкову послідовність (ключ).

Гаряча лінія

Можна показати, що для цієї системи умовна ентропія $H(M/C)$:

$$H(M/C) = H(K) - ld \log_2 m \tag{15}$$

l – довжина ключа.

d – надмірність алфавіту.

Визначимо умову, при якому реалізується безумовна стійкість, тобто знайдемо в символів криптограми, при якому не можна здійснювати криптоаналіз.

Задача криптоаналізу може бути визначена коли:

$$H(M/C) = 0$$

$$H(K) - l_0 d \log_2 m = 0$$

$$l_0 = \frac{H(K)}{d \log_2 m} \quad (16)$$

Фізично l0 – мінімальна кількість символів криптограми при правильному одержанні яких можна сподіватися на успішний криптоаналіз. Якщо l< l0,то система безумовно стійка. Це друга умова реалізації безумовно стійкою системи.

Лекція 4

Умови реалізації безумовно стійкою і обчислювально стійкою системою

1. Відстань одиничності для безумовно стійких (БС) і обчислювально стійких(ВР) КС.
2. Умова реалізації ВР КС.
3. Приклади.

Ціль: виявити умова реалізації ВР і БС КРС для моделі, приведеної на рис.3.1.

Задача оцінки відстані одиничності: КРА послідовно перехоплює криптограми З1,…Cn і вирішує задачу визначення значеннєвого змісту переданого Мі – повідомлення і ,як найбільш важливу, задачу визначення ключів Кj.

Очевидно, що його успіх у рішенні задач залежить від обсягу криптограм, що він одержав, при цьому КРА знаходиться в невизначеності $H(M/C)$.

$$0 \le H\left(M/C\right) \le H(M) \quad (1)$$

Найкращий випадок, якщо $H(M/C) = 0$.

По Шенону:

$$f\left(l/c_1, c_2, \ldots c_n\right) \quad (2)$$

l- загальний обсяг символів криптограми, який необхідно перехопити для рішення задачі. Очевидно, є l0 при який $H(M/C) = 0$, з іншої сторони він припустив, що для лінійних шифрів можна скласти і вирішити систему лінійних рівнянь і вона буде мати одне рішення, за умови, що є l0 незалежних коефіцієнтів для підстановки в цю систему. При цьому рішення самої задачі може бути дуже складним, але воно є – єдине. Для деякого класу лінійних (групових) шифрів, у яких використовуються природні мови (російська, англійська, С++, графіка) він одержав рівняння зв'язку $H(M/C)$ з ентропією джерела ключа Н(ДО), параметром l – довжиною k-m, d – надмірність мови.

$$I_K = \log_2 P(K_i)$$

$$H(K) = \sum_{i=1}^{n_K} P(K_i) \log_2 P(K_i) \quad (3)$$

$$H(M/C) = H(K) - ld \log_2 m \quad (4)$$

Апостеріорна ентропія $H(M/C)$ визначається через умовну апостеріорну імовірність $P(M_i/C_j)$.

$$H(M/C) = -\sum_{i=1}^{n_m} \sum_{j=1}^{n_c} P(C_j) P\left(M_i/C_j\right) \log_2 P(M_i/C_j) \quad (5)$$

$$H\left(M/C_j\right)=-\sum_{i=1}^{n_M} P\left(M_i/C_j\right)\log_2 P\left(M_i/C_j\right) \quad (6)$$

$$I_{m/c}=\log_2 P\left(M_i/C_j\right)$$

$H(M/C)$ можна розрахувати по (5), знаючи статистику P(Cj) і знаючи статистику $P(M_i/C_j)$.

Під надмірністю d розуміється ступінь корельованості (залежності) символів у мові і не порівняно ймовірностні їхньої появи в повідомленні.

$$d=\frac{H_0(M)-H(M)}{H_0(M)} \quad (7)$$

H0(M) – ентропія мови, де всі символи порівняно ймовірностні і незалежні.

$$P(M_1)=P(M_2)=....=P(M_m)=\frac{1}{m} \quad (8)$$

$$H(M)=-\sum_{i=1}^{n_m}\frac{1}{m}\log_2\frac{1}{m}=\log m \quad (9)$$

$$H_0=\log m \quad (10)$$

$$H(K)-ld\log_2 m=0 \quad (11)$$

$$l_0=\frac{H(K)}{d\log_2 m} \quad (11)$$

$$l_0=\frac{H(K)}{d} \text{ (якщо m=2)} \quad (12)$$

Приклад 1.

Знайти l0 для реального повідомлення на укр. яз., за умови, що джерело ключів містить:

$$\{K\}\Rightarrow 2^{128}=N_K$$

d=0,4

$$H(K)=\log_2 N_K=\log_2 2^{128}=128$$

$$l_0=\frac{128}{0{,}4}=320$$

Приклад 2.

Знайти l0 для безумовного шифру:

$$l_0=\frac{\log N_K}{d\log m}=\frac{\log m_K^{l_K}}{d\log m}=\frac{l_K\log m}{d\log m}$$

$l_K\geq l_m$ $\qquad N_K=m_K^{l_K}=m_K*m_K****m_K=m_K^{l_K}$

$$l_0\geq\frac{l_m\log m_K}{d\log m} \qquad m_K=m \quad (13)$$

$$l_0\geq\frac{l_m}{d} \qquad 0\leq d\leq 1 \quad (14)$$

Для безумовно стійкої системи l0 не менше довжини повідомлення, і не менше довжини ключа.

Для успішного криптоаналізу КРА повинний одержати не менш чим lк символів, тобто весь ключ.

Можна показати, що іншою умовою безумовної стійкості є вимогу:

$$H(K) > H(M)$$

Доведемо, думаючи, що алфавіти Н(ДО) - m_K , а Н(М) - m^{l_M} .

Покладемо, що $m_K = m_M$.

$$N_K = m^{l_K} \qquad (15)$$

$$N_M = m^{l_M}$$

Nk – у ключів

NM – у повідомлень

$$P(K_i) = m^{-l_K} \qquad P(M_i) = m^{-l_m}$$

$$H(K) = \log_2 N_K = \log_2 m^{l_K} = l_K \log_2 m$$

$$H(M) = \log_2 N_M = l_M \log_2 m$$

$$\boxed{l_K \log m_K \geq l_m \log m_M} \qquad (16)$$

$$l_M \leq l_K \qquad (17)$$

Приклад 3.

Визначити кількість символів ключа (обсяг ключів), які потрібно розіслати ДО1 і ДО2, зв'язаних між собою каналом зі швидкістю V=2Мг біт/сек, вони працюють протягом року безупинно.

$$l_M = 2 * 10^6 \, бит/сек * 3{,}11 * 10^7 = 6 * 2 * 10^{13} \, бит/год$$

$$n_Д = \frac{6{,}2 * 10^{13}}{5 * 10^9} \approx 1{,}2 * 10^4$$

Висновок: на цьому прикладі ми переконуємося, що хоча БС – систему теоретично реалізувати нескладно, але складно на практиці, у зв'язку з цим на практиці застосовують обчислювально – стійкі системи.

ВР КС – така КС, для якої tб набагато більше tци (цінності інформації).

$$t_б \geq t_{ци} \qquad (18)$$

У обчислювально стійких криптосистемах замість ключової послідовності Кі використовують Гі.

$$K_i \to Г_i$$

$$Г_i = \varphi(K_j) \qquad (19)$$

$$l_{K_j^u} = 56 - 25 біт$$

$$\underline{C_i = (M_i + Г_i) \bmod m} \qquad (20)$$

Пристрій чи алгоритм, що формує Гі, тобто реалізує функцію φ, називається шифратором, необхідний ключ довжини 100 – 1000 біт l_{K_u} .

Для такої системи Гі повинна задовольняти ряду вимог:

1) мати свідомо заданий період ($l_Г \geq l_{gm}$), 2^{128} і більш, 10^{76} символів.

2) $Г_i = \varphi(K_i)$ повинна мати складний закон формування ключа, інакше погана структурна скритність.

$$S_Г = \frac{l_H}{L_n} \to 1 \qquad (21)$$

$$l_H \to L_n$$

L_n - повний період.

3) відновлюваність Г, простору і часу.
4) однозначність формування Г і мінімальна складність функції φ.

Лекція 5

Обчислювально стійкі і доказово стійкі криптосистеми, їхня реалізація

1. Класифікація і характеристика.
2. Афіні шифри.
3. Потокові шифри.
4. Блокові і складені шифри.

Застосовувані на практиці криптоперетворення розділяють на 2 класи по стійкості:

1. обчислювально стійкі.
2. ймовірно стійкі (доказово стійкі).

Основним показником, по якому оцінюються такого роду системи є безпечний час:

$$t_б \geq t_{ци} \tag{1}$$

$$t_б = \frac{N_{вар}}{\gamma k} P_P \tag{2}$$

Nвар – кількість команд, операцій для рішення задачі криптоаналізу.

γ - продуктивність криптосистеми, вар/сек.

RSA: N=P*Q (3)

k – коефіцієнт кількості сек/рік $3{,}1 * 10^7 \, сек / год$

Pр – імовірність рішення задачі.

$$Y = \Theta^x (mP) \tag{4}$$

x-?

ВР і ДС повинні задовольняти (1). До доказово стійких перетворень відносять перетворення з відкритими ключами, з відкритим поширенням ключів і т.д. У цих системах задача криптоаналізу полягає в рішенні якоїсь іншої математичної задачі. Обчислювально стійкі системи реалізуються за рахунок застосування симетричних криптоперетворень.

$$C_j = F^+ (M_i, K_i^З, P_r) \tag{5}$$

$$M_i = F^- (C_j, K_j^p, P_r) \tag{6}$$

У симетричних криптосистемах ключ зашифрування або збігається з ключем розшифрування, або обчислюється один з іншого з поліноміальною складністю.

$$K_j^З = K_j^З \tag{7}$$

Поліноміальна складність

Нехай n – розмірність вхідних даних, що підлягають криптоперетворенню і нехай t(n) є складність перетворення цих даних у сек. тактах, командах. Складність називають поліноміальної, якщо вона представлена:

$$t^Г(n) = \sum_{\nu=1}^{z} C_\nu n^{C_\nu} \tag{8}$$

C_ν - набір констант.

$t^e(n) = C_1^{n^{C_2}}$ - експонентна складність (9)

В даний час як функцію f реалізуючої криптоперетворення використовуються афінні шифри.

Афінне перетворення – перетворення, яке можна одержати комбінуючи рухи, дзеркальні відображення і гомотепію в напрямку координатних осей.

Гомотепія – перетворення простору чи площини щодо точки по направляючим осях з коефіцієнтами.

До афінних шифрів відносяться чи шифри перетворення зрушення, лінійні шифри, афінних шифри. Нехай Mi – символ чи повідомлення цифри (буква), нехай також a і s ключі, причому:

$$0 \le s < M \qquad 0 < a < n$$

НСД(a, n)=1

то існує оборотний афінний шифр із функцією зашифрування:

$$C_i = E(M_i) = (a * M_i + S) \bmod n \tag{10}$$

n – модуль перетворення шифру, розмір алфавіту.

і - функція перетворення.

$$M_i = Д(C_i) = (a' * C_i + S') \bmod n \tag{11}$$

$$a' = a^{-/}(\bmod n) \tag{12}$$

$$S' = a^{-/}(-S) \bmod n \tag{13}$$

Якщо S=0 у шифрі, то такий шифр називається лінійним афінним шифром, якщо в шифрі a=1, то шифр називається шифром зрушення. Більшість шифрів вкладається в клас афінних шифрів.

У потокових криптоперетвореннях об'єктами взаємодії є символи повідомлення Mi і символи ключа Kj, причому з використанням символів ключа формується Гі.

$$\text{Mi}, \quad \text{Kj}, \quad \Gamma_i = \varphi(K_j)$$

$$C_i = (M_i * \Gamma_i) \bmod m \tag{14}$$

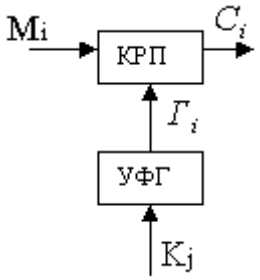


Рис 5.1

* - множення, + , - ;

Розшифрування:

$$M_i = (C_i * \Gamma_i) \bmod m \tag{15}$$

При обчисленні необхідно строго синхронізувати по і, тобто: Гі при розшифруванні і зашифруванні та сама.

М – ічне шифрування (по mod).

Приклад:

$$\left.\begin{aligned} C_i &= (M_i + \Gamma_j) \bmod M \\ M_i &= (C_i - \Gamma_i) \bmod M \end{aligned}\right\} \tag{16, 17}$$

$$0 \le M_i, \ \text{C}_\text{i}, \ \Gamma_\text{i} < m$$

Двійкове гамування

$$\begin{cases} C_i = M_i \oplus \Gamma_i & (18) \\ M_i = C_i \oplus \Gamma_i & (19) \end{cases}$$

Гі повинна породжуватися псевдовипадковим чи випадковим процесом. Реалізація процесу повинна залежати від вихідного ключа.

Правильне розшифрування в (18), (19) за умови, що відправник і одержувач використовують той самий ключ, вони можуть сформувати однакові гами. Необхідно забезпечити синхронізацію по і.

Блоковими перетвореннями називаються такі шифри, при яких інформація М поділяється на блоки Мі по l_{M_i} в кожнім із блоків. Кожний із блоків зашифровується з використанням того самого ключа.

Блокове шифрування можна реалізувати за рахунок:

1) використання операцій перестановки символів у блоці за законом ключа;
2) підстановки (чи заміни) замість символів повідомлення інших символів, що задаються ключем;
3) за рахунок використання в загальному випадку афінного перетворення (11), (12), якщо Мі – символи розглядати як блоки;
4) за рахунок використання операції керування цикл. зрушенням блоку за законом ключа

Шифр монопідстановки – задається ключем у виді входу і виходу. У рядку вхід записується вихідний алфавіт. У рядку вихід записується одна з можливих комбінацій (символи алфавіту в довільному порядку).

Вхід: а б в г....

Вихід: я д щ з …...

Найважливішою характеристикою всіх розглянутих шифрів є кількість вихідних ключів, що дозволені в системі.

На рис.5.2 приведений алгоритм блокового симетричного шифрування (чи складеного шифру).

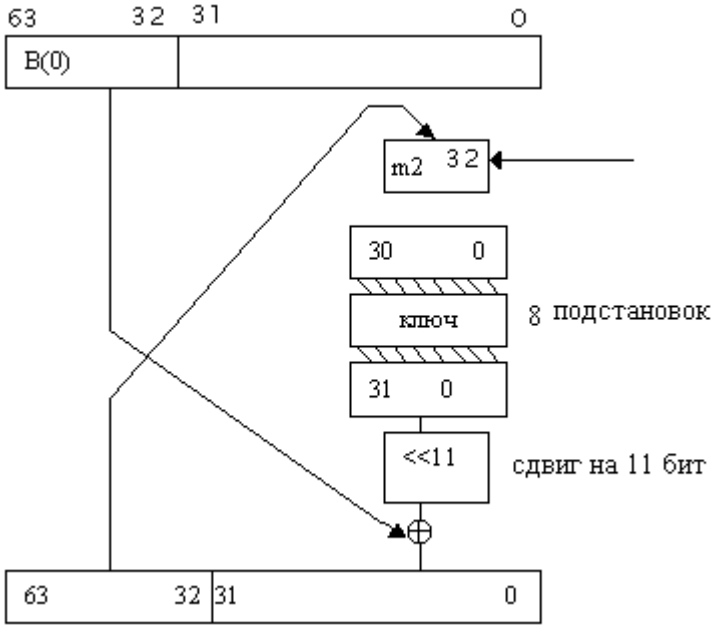


Рис.5.2

Лекція 6

Алгоритми і засоби формування ключів і паролів.

1. Вимоги.
2. Лінійний рекурентний регістр. Його властивості.
3. Лінійний конгруентний генератор.
4. Проблемні питання.

Обчислювально стійкі системи реалізуються на основі використання вихідних ключів визначеної довжини, тоді:

$$\Gamma_i = \varphi(K_j^u, P_r) \quad (1)$$

$$\begin{cases} C_i = M_i \oplus \Gamma_i & (2) \\ M_i = C_i \oplus \Gamma_i & (3) \end{cases}$$

У реалізації системи шифрування (2), (3) найбільш складною задачею є формування Гі, що задовольняє наступним умовам:

1. $$L_n \geq L_g \quad (4)$$

Lg – min припустиме значення.

2. Гі повинна володіти високою структурною скритністю.

Рис.6.1

структурна скритність - $$Sc = \frac{l_H}{l_n} \quad (5)$$

lн – мінімальна кількість біт з послідовності, при знанні яких можна визначити закон формування послідовності φ.

Кращий випадок, якщо $Sc \to 1$ (якщо $l_H = l_n$, Sc = 1) – називається абсолютно (зовсім) потайливий. Це може бути тільки фізичний випадковий процес. У житті за рахунок перетворення ? можна досягти тільки кінцевих значень структурної скритності.

3.Відновлюваність гами в просторі і часі. Закон ? може бути повторений при введенні ідентичних вихідних ключів і параметрів.

4. Апаратна, програмна чи апаратно – програмна реалізуємість із припустимою складністю.

У правилі (1) при формуванні Г в якості вихідних ключів повинні використовуватися чисто випадкові послідовності і джерело ключів повинне породжувати K_j^u - ключі випадково, порівняно ймовірно, незалежно й однорідно. Тільки при цьому умові забезпечується обчислювальна складність криптоперетворення.

5. Найбільш загальною характеристикою Гі і джерела ключів є tб.

$$t_б = \frac{N_{вар}}{\gamma K} P_T \quad (6)$$

де Nвар – кількість варіантів, що КРА повинний виконати, реалізуючи криптоаналіз.

γ – продуктивність його системи;

Рт – імовірність, з якою повинний бути успішно зроблений криптоаналіз.

tб – мат. чекання часу злому системи (якщо Рт = 1).

Задача:

Нехай мається генератор псевдовипадкової послідовності.

$$L_n = 2^{256} - 1; \quad \text{частота} : 10^{12}\,Гц$$

Знайти t у проміжку якого цей генератор сформує послідовність на всьому періоді.

$$t = \frac{2^{256} - 1}{10^{12} * 3 * 10^{7}} = \frac{10^{76,8}}{3 * 10^{19}} = 3,3 * 10^{56,8} \approx 10^{57} \text{ лет}$$

Один з генераторів, де завжди виконується 1-і умова – лінійний рекурентний регістр (лінійний автомат).

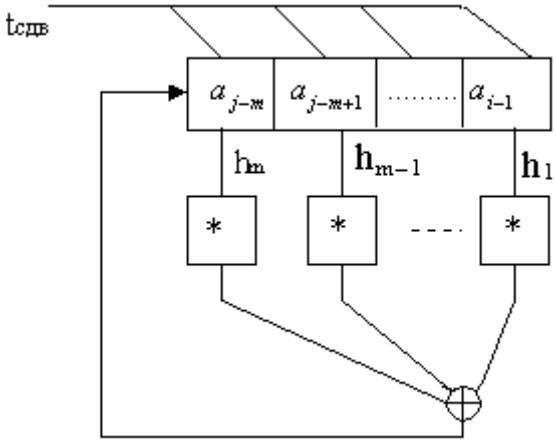


Схема приведена на рис.6.2.

Автомат складається з m – ячеєк пам'яті, що утвоюють регістр, що рухає. На цей регістр подаються символи зрушення fсдв. При подачі кожного імпульсу на вихід зчитується aj – символ, при цьому всі символи в ячейках пам'яті зрушуються ліворуч праворуч. Крім того, ці ж імпульси збільшуються на з і результат множення складається по mod2. Результат додавання записується в aj – m осередок і т.д. При подачі наступних імпульсів зрушення робота повторюється. Основною задачею є вибір вектора h. Якщо h вибирати відповідним чином, то такий автомат буде генерувати послідовність з періодом. $2^m - 1$, m - кількість розрядів.

$$L_n = 2^m - 1$$

Достатньою умовою забезпечення максимального періоду є вибір h відповідно до коефіцієнтів примітивного полінома m – ступеня.

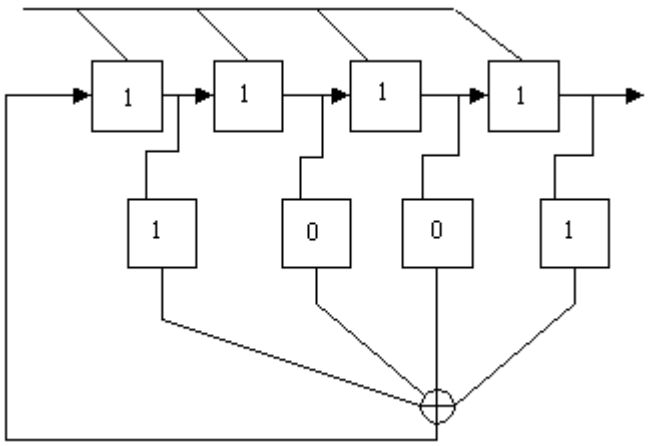
$$h \to f(x) = h_m x^m + h_{m-1} x^{m-1} .....h_1 x + h_0 \qquad (7)$$

Примітивним називається поліном, що породжує розширене поле $GF(2^m)$. У розширеному полі еквівалентному простого числа є примітивний поліном f(x).

Нехай $f(x) = x^4 + x + 1$

$1 * x^4 + 0 * x^3 + 0 * x^2 + 1 * x + 1$

$h_4 \quad h_3 \quad h_2 \quad h_1 \quad h_0$



Запишемо послідовність 4 біт:1111

1. 1111 + зрушення вправо $2^m - 1 = 2^4 - 1 = 15$
2. 0111
3. 1011
4. 0101
5. 1010
6. 1101
7. 0110
8. 0011
9. 1001
10. 0100
11. 0010
12. 0001
13. 1000
14. 1100
15. 1110
16. 1111

Властивості ЛРР.

1. Якщо поліном примітивний, то період $L_n = 2^m - 1.$
2. На періоді з'явиться на одну одиницю символів більше, ніж нулів.
3. Максимальна серія з однакових символів 1-послідовностей буде дорівнює m, 0 – m-1.

Регістр формує хорошу послідовність, за винятком: послідовність володіє низькою структурною скритністю. Для розкриття закону формування необхідно перехопити 2m підряд розташованих символів (бітів).

$$Sc = \frac{2m}{2^m - 1} \tag{8}$$

ЛКГ працює за правилом:

$$X_n = (ax_{n-1} + c) \bmod 2^m$$

Початковий стан установлюється за рахунок завдання хо, з, а також правильного вибору а. хо, з можуть бути випадковими, але а вибираємо спеціальним образом (воно не парне), якщо а обране правильно, те генератор формує послідовність 2^m.

Лекція 7

Системи з відкритими ключами і відкритим розподілом ключів. (частина 1)

1. RSA з відкритими ключами.
2. Алгоритм криптоперетворення.
3. Генерація ключів.
4. Оцінка стійкості і складності.

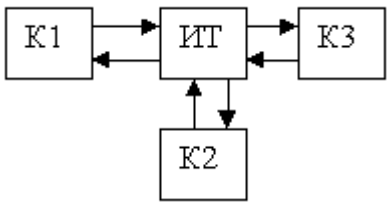


Рис.7.1.

Необхідно реалізувати систему взаємної недовіри і взаємного захисту, кожний з користувачів нікому не довіряє свої ключі і параметри і хоче мати гарантію компенсацію втрат, якщо його обдурять.

DES – алгоритм, у ньому :

$$K_j^З = K_j^p \quad (1)$$

$$I = \sum C_1 n^{C_2} \quad (2)$$

RSA – (Рівер, Шаміль, Отаман) – складно обчислити ключі один з іншого.

$$K_j^З \neq K_j^p \quad (3)$$

Сутність алгоритму - він є блоковим, у ньому повідомлення М розбивається на блоки Мі, з довжиною блоку $l_j \geq l_g$ (768 біт мінімум), реально 1024, 2048.

$$C_i = M_i^{E_K} (\mathrm{mod}\, N) \quad (4)$$

E^K - ключ прямого перетворення $E^K = K^З$.

$$N = P * Q \quad (5)$$

P, Q – великі прості числа.

$$l_p + l_a = l_N$$

Дешифрування за правилом:

$$M_i = C_i^{Д_K} (\mathrm{mod}\, N) \quad (6)$$

Дк - ключ зворотного перетворення $Д^K = K^P$.

Підставимо (4) у (6):

$$M_i^1 = M_i^{E_K Д_K} (\mathrm{mod}\, N)$$

Використовуючи теорію порівняння:

$$E_K Д_K = 1 (\mathrm{mod}\, \varphi(N)) \quad (7)$$

Якщо (7) має єдине рішення, тобто існує єдина пара $E_K Д_K$, то такий шифр є однозначним.

Генерація ключів (задачі)

1. Генерація випадкової пари $E_K Д_K$.
2. Генерація P і Q, що задовольняє умові (5).
3. RSA відноситься до системи з відкритими ключами, що порозуміється тим, що ключі E_K и $Д_K$ поділяються на двох частин.

с E_K - з'являється конфіденційним (особистим).

$Д_K$ - відкритий (публічний) для шифрування навпаки.

Усі параметри (N,P,Q) також поділяються на 2 класи: N – відкритий, P,Q - конфіденційний (секретний).

Сутність моделі взаємної недовіри – кожен користувач генерує ключі сам собі. Особистий ключ залишає в себе і забезпечує його строгу конфіденційність. Відкритий ключ розсилає всім користувачам, з якими він зв'язаний. Він також забезпечує цілісність і дійсність відкритих ключів.

$E_K Д_K$ - повинні вибиратися з повної множини випадково, порівняно ймовірно і незалежно, повинні забезпечувати однозначну оборотність прямого зворотного перетворення.

$$1 \leq E_K Д_K < \varphi(N)$$

$$\varphi(N) = \varphi(P * Q) = \varphi(P) * \varphi(Q) * (P-1)(Q-1) \quad (8)$$

(7) можна звести до Діфантового рівняння:

$$ax+by=1 \quad (9)$$

Діафантове рівняння – нормоване, тому що праворуч коефіцієнт = 1, a, b – цілочисельні коефіцієнти, x, y – невідомі.

$$E_K Д_K = k * \varphi(N) + 1 \tag{10}$$

k – деяке невідоме число

E_K можна згенерувати випадково.

Діафант. рівняння має цілочисельне рішення, якщо a і b цілочисленні, і a ≥ b, a і b взаємно прості.

$$\begin{matrix} \varphi(N) * (-k) + E_K Д_K = 1 \\ a \quad x \quad b \quad y \end{matrix} \tag{11}$$

Одним з найбільш швидких рішень (11) є ланцюгові дроби.

$$\begin{cases} y = (-1)^{\mu} a_{\mu-1} \\ x = (-1)^{\mu} b_{\mu-1} \end{cases}$$

де ? – порядок ланцюгового дробу, a і b – параметри ланцюгового дробу.

Знаходимо параметри:

a/b представляється у виді ланцюгового дробу.

$$\frac{a}{b} = r_0 + \cfrac{1}{r_1 + \cfrac{1}{r_2 + \cfrac{1}{r_3 + \\ \quad \ldots \\ \cfrac{1}{r_\mu + 0}}}} \tag{12}$$

μ - порядок ланцюгового дробу, перший коефіцієнт, у якого залишок дорівнює 0.

$$\left.\begin{matrix} \frac{a_0}{b_0} = r_0 = \frac{r_0}{1} & a_0 = r_0 \\ & b_0 = 1 \end{matrix}\right\}$$

$$\left.\begin{matrix} \frac{a_1}{b_1} = r_0 + \frac{1}{r_1} = \frac{r_0 r_1 + 1}{r_1} & a_1 = r_0 r_1 + 1 \\ & b_1 = r_1 \end{matrix}\right\}$$

$$\begin{cases} a_\mu = r_\mu * a_{\mu-1} + a_{\mu-2} \\ b_\mu = r_\mu * b_{\mu-1} + b_{\mu-2} \end{cases} \tag{13}$$

При великих N – велике значення μ. $\mu \approx ⅓ N$.

Оцінка стійкості і складності

RSA – доказово стійка система (криптоалгоритм). Основною задачею для RSA є перебування ($E_K, Д_K$) і параметрів.

Кількість пар $E_K, Д_K$ для заданого N :

$$N_{кл} = \varphi(\varphi(N)) = \varphi((P-1)(Q-1)) \tag{14}$$

Очевидно, якщо P-1 і Q-1 d великі й у канонічному розкладанні мають мало співмножників, то кількість ключів буде максимізоване.

Числа P і Q повинні бути не просто простими, а сильними простими числами (у вузькому змісті), тобто мати вид:

$$P=2R+1 \tag{15}$$

P – просте

Зловмиснику доступний відкритий ключ E_K, він знає N, тоді він може знайти $Д_K$, якщо він довідається $\varphi(N) = (P-1)(Q-1)$, тобто P і Q. Основна його задача розкласти N на 2 співмножники P і Q. Ця задача називається факторізациею модуля.

RSA – доказово стійка система, тому що доказ стійкості зводиться до доказу складності розкладання N на 2 співмножники.

$$t_б = \frac{N_{вар}}{\gamma_k}$$

За останні 20 років математика працювала над рішенням задачі факторизації дуже великих чисел.

Теорії:

1. Теорія P-1, ?
2. Теорія Ленстри
3. Двійкове решето
4. Загальне решето числового поля

Для 4 –случаю

складність криптоаналізу оцінюється з використанням суб експоненціального алгоритму:

$$I = \exp(\delta(\log N)^{\nu}(\log\log N)^{-\nu}) \quad (16)$$

?, ? – параметри методу

δ=1,96 ν=1/3

I – кількість групових операцій, який треба виконати для факторизації методу N.

(частина 2)

1. Загальна характеристика.
2. Схеми розподілу ключів по відкритих каналах.
3. Оцінка стійкості.
4. Проблеми теорії і практики.

$$K^3 \neq K^p \quad (1)$$

Відняти один з іншого складно.

$$I = C_1^{n^{C_2}} \quad (2)$$

n – розмірність вхідних даних, для RSA – N – довжина модуля перетворення в бітах.

При спрямованому шифруванні параметри і ключі поділяють на 2 групи:

1. особисті (D_K, P_j, Q_j)
2. публічні (відкриті) (E_K, N_j), $N_j = P_j Q_j$

k – ий користувач генерує особисті і відкриті ключі і параметри.

ν – ий користувач шифрує M_i використовуючи:

$$C_i = M_i^{E_K} (\mathrm{mod}\, N_j) \quad (3)$$

розшифрувати її може k – ий користувач, тоді:

$$M_i = C_i^{D_K} (\mathrm{mod}\, N_j) \quad (4)$$

Для спрямованого шифрування:

1. Найбільш оптимальним методом для криптоаналізу є перехоплення повідомлення N_j и $\mathrm{E_K}$.
2. Факторизація модуля N_j (знайти P, Q).
3. Потім знайти

$$E_K D_K \equiv 1(\mathrm{mod}\,\varphi(N_j)) \tag{5}$$

$$\varphi(N_j) = (P_j - 1)(Q_j - 1) \tag{6}$$

$$I = \exp(\delta(\log N)^{\nu}(\log\log N)^{-\nu}) \tag{7}$$

δ, ν – параметри, залежать від методу факторизації.

Мається n – користувачів мережі, кожний з них генерує ключі своєї станції, частина з них може оголосити особистими чи конфіденційними, а частина може роздати користувачам мережі.

Треба виробити ключ зв'язку (захисту) інформації на сеанс, скориставшись відкритими каналами зв'язку. Наприклад: виробити K^3, K^p, у тому числі для симетричної системи. Зважується в полях Галуа.

Протокол, що одержав поширення вироблення загального секрету 2 користувачами – протокол Діфі – Хелмана.

Нехай маються користувачі А и В, один з них чи центр генерує пари чисел Р, Θ.

Р – просте число.

Θ – первісний елемент, що породжує поле GF(p).

$$\Theta_{\nu} \to GF(p)$$

$$\Theta_{\nu}^{i}(\mathrm{mod}\ p), \qquad i = 0, P-1$$

Θ – просте число, з інтервалу 0, Р-1, що будучи зведене в ступінь дає структуру простого поля, тобто з'являться всі числа один раз.

$$P \in \{P\} \qquad \mathrm{j} = \mathrm{n_p}$$

Кожен користувач генерує ключі Х с довжиною l.

$$X_A \quad l_{\mathrm{X_A}} \qquad\qquad \mathrm{X_B} \quad l_{X_B}$$

Після цього обчислюють відкритий ключ:

$$Y_A = \Theta_{\nu}^{X_A}(\mathrm{mod}\,P_j) \qquad Y_B = \Theta_{\nu}^{X_B}(\mathrm{mod}\,P_j) \tag{8}$$

Після цього розсилають відкриті ключі по відкритих каналах один одному, забезпечуючи при цьому їх цілісність і дійсність. Кожний з них може обчислити загальний секрет:

$$Y_{AB} = Y_B^{X_A}(\mathrm{mod}\,P_j)$$

$$Y_{AB} = \Theta_{\nu}^{X_B X_A}(\mathrm{mod}\,P_j) \tag{9}$$

$$Y_{BA} = Y_A^{X_B}(\mathrm{mod}\,P_j) = \Theta_{\nu}^{X_A X_B}(\mathrm{mod}\,P_j) \tag{10}$$

$$Y_{AB} = Y_{BA} \tag{11}$$

Значить загальний секрет може бути використаний як ключ симетричного шифру. Стійкість цієї схеми:

Основна задача КРА – знайти ХА, ХВ. Простіше всього угадування ХА, ХВ, захиститися від цього можна вибравши велику довжину ключа і виробити їх випадково.

$$P_y \le P_g = \frac{1}{2} l_X$$

Т.к. $Y_B, \Theta_{\nu}, \mathrm{P_j}$ - відкриті параметри, те КРА знаючи їх може спробувати вирішити рівняння:

$$Y_j = \Theta_{\nu}^{X_i}(\mathrm{mod}\,P_j)$$

$$X_i = \log_{\Theta_{\nu}} Y_i(\mathrm{mod}\,P_j) \tag{12}$$

(12) – проблема дискретного логарифма (дискретне логарифмічне рівняння - ДЛР).

Стійкість схеми Диффи – Хелмана визначається складністю рішення дискретного логарифмічного рівняння виду (12).

Для методу розрахунку загального числового поля складність рішення носить субекспоненціальний характер і може бути оцінена співвідношенням (7) зі своїми параметрами ?, ?.

Є ряд загальних проблем реалізації і застосування цих алгоритмів.

1. Проблема генерації великих простих чисел відповідної довжини.

$$l_P = 512 \div 2048 \quad \text{бит}$$

$$2^{512} \div 2^{2048}$$

2. Складність обчислень.

$$1 < \Theta_\nu < P - 1$$

$$l_\Theta \le l_P$$

3. Арифметична багаторазова точність. Складність цих перетворень дуже велика, набагато більше, ніж у симетричних криптосистемах.

4. $$E_K D_K \equiv 1 (\mathrm{mod}\, N_j)$$

Загальні проблеми: перетворення в кільцях і полях

Застосування методів RSA і Діфі – Хелмана привело до появи нових математичних методів криптоаналізу:

- методи факторизації

$$N_j \Rightarrow P_j Q_j$$

- задача рішення ДЛУ:

$$X_i = \log_{\Theta_\nu} Y_i (\mathrm{mod}\, P_j)$$

для (1) метод Поларда (P-1 і ρ), методи Ленстрі, двійкове решето, загальне і спеціальне решето числового поля.

Протиріччя дозволяється за рахунок збільшення N_j, P_j, але збільшується складність обчислення відкритого ключа, зменшується швидкість шифрування. Протиріччя дозволяється за рахунок виконання рівнобіжних перетворень у групах точок еліптичних кривих над полями.

Лекція 8

Криптоперетворення в групах точок еліптичних кривих

1. Поняття еліптичної кривої над полем Галуа.
2. Метрика операцій на ЕК.
3. Приклади.

Складність перетворень у ЕК:

$$I \cong \sqrt{kn} \tag{1}$$

де n – порядок базової точки на ЕК (період).

Ця складність набагато більше, ніж субекспоненціальна складність від $I(\delta, \nu)$.

$$I(\delta, \nu) = e^{\delta (\ln N)^\nu (\ln \ln N)^{1-\nu}} \tag{2}$$

$$\uparrow I \rightarrow \uparrow (N, \uparrow E_K)$$

$$C_i = M_i^{E_K} (\mathrm{mod}\, N)$$

Кубічна ЕК в афінном базисі над простим полем має вид:

$$y^2 \equiv (x^3 + ax + b) \bmod P \quad (3)$$

(x, y) - точки ЕК,

а, б – параметри ЕК

$$2a^3 + 27b^2 \neq 0 (\mathrm{mod}\, P) \quad (4)$$

(x_i, y_i) - належить ЕК, якщо ця пара чисел задовольняє порівнянню (3). Над розширеним полем $GF(2^m)$ рівняння ЕК має вид:

$$y^2 + xy \equiv (x^3 + ax^2 + b) (\mathrm{mod}\, f(x), 2) \quad (5)$$

(x_i, y_i) - точка на ЕК,

а, б – коефіцієнти (параметри) ЕК

f(x) – примітивний поліном над полем $GF(2)$.

$$f(x) = x^m + h_1 x^{m-1} + h_2 x^{m-2} + \ldots + h_{m-1} x^1 + h_m \quad (6)$$

Поліном називається примітивним, якщо він що не приводиться, а з іншої сторони породжує поле $2^m - 1$.

У рівнянні (5) x_i и y_i, а також a і b являють собою m-бітні вектора в поліноміальному чи нормальному базисах, зокрема, у поліноміальному базисі x, y, a, b, є поліномами не вище m - ступеня, тому всі операції виконуються не вище m – ступеня.

Є 3 – мірне перетворення ЕК, називається проективною геометрією (представлення). У проективній геометрії кожна точка задається - X,Y,Z – дозволяє прискорити проведення операцій.

$$Y = \Theta_v^x (P) \quad (7)$$

- еквівалент у групах точок ЕК заміняється скалярним множенням.

$$Q = d * G (\mathrm{mod}\, P) \quad (8)$$

у (8) d – число, G – базова точка на ЕК (x_g, y_g) породжує групу точок n – порядку.

чи

$$Q = d * G(mf(x), 2) \quad (9)$$

у (9) d – особистий секретний ключ = x.

$$Q = \underbrace{G + G + G + \ldots G}_{d} \quad (10)$$

При виконанні (10) виділяють 2 операції: операція подвоєння – складається 2 однакові точки, і операція додавання – складаються 2 різні точки.

$$P_1 = (x_1, y_1) \qquad P_2 = (x_2, y_2) \quad (11)$$

на ЕК сума цих точок:

$$P_1 + P_2 = (x_1, y_1) + (x_2, y_2) = P_3 = (x_3, y_3) \quad (12)$$

$$P_3 = 2P_1 = (x_3, y_3)$$
$$2P_2 = (x_3, y_3) \quad (13)$$

Метрика операцій на ЕК

$$\begin{cases} x_3 = (\lambda^2 - x_1 - x_2)mp \\ y_3 = (\gamma(x_1 - x_3) - y_1)(mp) \\ \lambda = \dfrac{y_2 - y_1}{x_2 - x_1}(mp) \end{cases} \quad (14) \quad (14.3)$$

(14) – визначає метрику додавання 2 точок.

точно також для подвоєння, але (14.3) заміняємо (15):

$$\lambda = \frac{3x_1 + a}{2y_1} mp \quad (15)$$

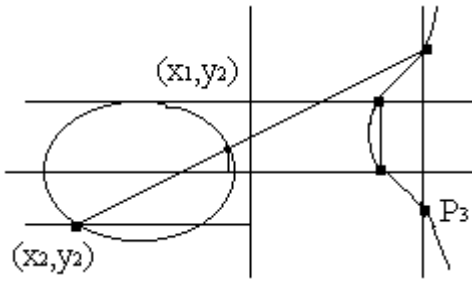


Рис.14.1

на ЕК є точка ОБ – нейтральний елемент, точка нескінченності.

Приклади:

Нехай мається ЕК.

$y^2 = (x^3 + x + 1) \bmod 23$

а = 1, б = 1, P = 23

1. Перевірити, що наступні точки: (1,7), (1,16), (3,10), (3,13), (4,0), (5,4), (5,19), (6,4), (6,19), (7,11), (7,12), (9,7), (9,16), (17,3), (17,20), (18,20), (19,5), (13,16) належать ЕК.

P1=(3, 10) P2=(9, 7)

Знайти $P_1 + P_2 = P_3$.

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}(mp) = \frac{7-10}{9-3}(m23) = -\frac{3}{6}(m23) = -\frac{1}{2}(m23) = \frac{22}{2}(m23) = 11$$

$$x_3 = (121 - 3 - 9)m23 = 109(m23) = 17$$

$$y_3 = (11(3-17) - 10)m23 = (-11*14 - 10)m23 = -164(\bmod 23) = 20$$

P3=(17,20)

(частина 2)

1. Афінні і проективні базиси.
2. Приклади перетворень.
3. Порівняння перетворень у полях, кільцях, еліптичних групах.

Відомо 2 представлення груп точок ЕК, 2 базиси: афінний і проективний.

Афінний базис

Для поля $GF(2^m)$, $q = 2^m$

$$y^2 + xy \equiv x^3 + ax^2 + b(\mathrm{mod}\, f(x),2) \quad (1)$$

де x_i, y_i - точки ЕК $(x_i, y_i) \in E(GF(2^m))$

а, б – параметри ЕК, $b \neq 0(mf(x),2)$

У порівнянні (1) x_i, y_i, а також a, b – коефіцієнти, є поліномами не вище m – порядку.

m

2

$$f(x) = h_{m-1}x^{m-1} + h_{m-2}x^{m-2} + h_1x^1 + h_0$$

$\forall h_i + GF(2)$

m≥160 $GF(2^{160})$ и вище, зараз реально (2^{192}) и вище.

Афінний базис вимагає великої обчислювальної складності.

$$Q = d * G(mf(x),2)GF(2^m) \qquad \mathrm{q} = 2^{\mathrm{m}} \quad (2)$$

$G \Rightarrow (x_G, y_G)$ - базова точка.

d – особистий секрет ключа $d \in [1, n-1]$

n – порядок (період) базової точки G.

$$n * G(mf(x),2) \equiv 0$$

Для зменшення чи складності підвищення швидкості використовується проективний базис:

X,Y,Z

при цьому перехід з афінного представлення в проективний:

$$x = \frac{X^2}{Z^2} \qquad \mathrm{y} = \frac{Y}{Z^3} \quad (3)$$

підставимо (3) у (1).

$$\frac{Y^2}{Z^6} + \frac{X}{Z^2} * \frac{Y}{Z^3} \equiv \frac{X^3}{Z^6} + \frac{aX^2}{Z^4} + b(mf(x),2) \qquad Z \neq 0$$

$$Y^2 + XYZ \equiv X^3 + aX^2Z^2 + bZ^6(mf(x),2) \quad (4)$$

(4) задає ЕК над полем $GF(2^m)$ у проективному базисі.

(X,Y,Z) – кожна точка задається трьохмірно.

Метрика 2 над полем $GF(2^m)$

Нехай відомі координати 2 точок:

$$P_1 = (x_1, y_1) \qquad P_2 = (x_2, y_2) \quad (x_i, y_i) \in GF(2^m)$$

$$P_3 = P_1 + P_2 = (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

$$P_3 = 2P_1 = P_1 + P_1 = (x_3, y_3) \quad (5)$$

$$x_3 = (\lambda^2 + \lambda + x_1 + x_2 + a)\,\mathrm{mod}(f(x),2) \quad (6)$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1(mf(x),2) \quad (7)$$

$$\begin{cases} x_3 = \lambda^2 + \lambda + a(mf(x),2) \\ y_3 = x_1^2 + (\lambda+1)x_3(mf(x),2) \\ \lambda = \left(x_1 + \frac{y_1}{x_1}\right)(mf(x),2) \end{cases} \quad (8)$$

У (7), (8) усі параметри – поліноми не вище m– того ступеня.

F(x)- примітивний поліном над $GF(2^m)$.

Примітивність $\Theta_\nu^i(mf(x))$ - max період поля буде 2^{m-1} елементів.

Лекція 9

Загальносистемні параметри перетворень на ЕК

1. Методи побудови простих чисел і примітивних поліномів.
2. Побудови і властивості базових точок на ЕК.
3. Характеристика методів, визначення порядку в ЕК.

1) q – порядок поля

$q = p,\ 2^m,\ p^m$

2) $E(GF(q))$ a, b, И

3) $G = \{x_G, y_G\}$, n – просте число, порядок точки G.
n(modq)≡0

4) U повинно бути майже простим,

$U = h*n \qquad h = 2,4,8,16$

P $2^{160} \div 2^{4096}$

Усі методи побудови простих чисел можна розділити на 3 класи:

1) аналітичні
2) "псевдопрості"
3) гіпотетичні (на основі гіпотез)

До аналітичного відносяться методи, на основі яких можна побудувати строго простt число.

Метод спробного розподілу

Що перевіряється m поділяється послідовно на всі прості числа менше $\sqrt{m}$.

$$m_i < \lfloor \sqrt{m} \rfloor \quad (1)$$

Якщо m не поділяється на всі m_i, то воно просте, тобто:

m = p

$$n_p = \lfloor \sqrt{m} \rfloor / \ln \lfloor \sqrt{m} \rfloor$$

Цей метод рекомендується для коротких довжин, чи як додатковий метод. Прості числа повинні закінчуватися 1, 3, 7, 9.

Числа Эйлера

$$m = 2^K - 1$$

Де k-просте, простими є 2,3,5,7,11,13,17,19,31,107,127,607,…19997і т.д.

$2^{2^n} + 1, \quad n = \overline{0,1,3,4}$ для таких n- просте.

Теорема Люка

Для числа m, для якого відомо канонічне розкладання m-1 справедливе теорема Люка:

Якщо для (a, m) $a^{m-1} \equiv 1(\mathrm{mod}\, m)$, то m-просте.

$$a^{\frac{m-1}{\alpha_i}} \neq 1(\mathrm{mod}\, m)$$

$$m - 1 = \alpha_1^{x_1} \alpha_2^{x_2} .....$$

Перший метод базується на теоремі Ферма.

$$a^{m-1} \equiv 1(\mathrm{mod}\, m)$$

$$(a^{m-1}) \equiv 0(\mathrm{mod}\, m)$$

$$\left(a^{\frac{m-1}{2}} - 1 \right)\left(a^{\frac{m-1}{2}} + 1 \right) \equiv 0(\mathrm{mod}\, m)$$

Тест Лемана

1) $a^{\frac{m-1}{2}} \equiv 1(\mathrm{mod}\, m) \qquad a^{\frac{m-1}{2}} \equiv -1(\mathrm{mod}\, m)$ (2)

Якщо a – первісний елемент, то $a^{m-1} \equiv -1(\mathrm{mod}\, m)$ генерується t-чисел a, взаємнопростих з m, потім для кожного a здійснюється перевірка.

2) Якщо на всіх t – перевірках одне з умов виконується, те число m можна вважати псевдопростим, це число з імовірністю $P_C \leq 2^{-t}$ того, що число не просте.

Примітивні поліноми табульовані і відомі усі до 2000 ступеня.

Метод гіпотез не застосовується, тому що базується на недоведених гіпотезах.

Побудови і властивості базових точок на ЕК

Базовою точкою на ЕК може вважатися кожна (x_g, y_g)- точка, що з однієї сторони задовольняє рівнянню ЕК, а з іншої має порядок n.

$nG(\mathrm{mod}\, q) \equiv 0$, n- просте

G – повинна бути випадкової.

$n > 2^{160}$ nh=И h-k – фактор=2,4,8

Найбільш складна задача побудови ЕКіз заданими значеннями И =nh. Треба знайти параметри (a, b, q), а також n, И, зв'язані

4) (a, b, q, n, И) – випадкові.

Відомо 3 методи побудови:

1. метод комплексного множення
2. метод Скуффа
3. метод через підполя

Окремий випадок, якщо $q = 2^m$. Якщо m розкладається на співмножники,

$m = m_1 * m_2 \; m_1 = 10$ (порядок)

$E(2^{m_1})E(2^{m_2})$ за методикою перерахувати для випадку m.

Лекція 10

Методи побудови загальносистемних параметрів

1. Метрика додавання і подвоєння в проективних координатах.
2. Тест Рабінера – Міллера побудови простих чисел.
3. Приклади розшифрування в розширених полях.

Рівняння кривої в проективних координатах

$$Y^2 + XYZ \equiv x^3 + aX^2Z^2 + bZ^6 (\mathrm{mod}\, f(x),2) \qquad (1)$$

Можна показати, що операції додавання і подвоєння для кривої (1) можуть бути обчислені в наступному виді:

$$P_1 = (X_1, Y_1, Z_1) \qquad P_2 = (X_2, Y_2, Z_2) \qquad (X_3, Y_3, Z_3) = P_1 + P_2 = P_3$$

$$U_0 = X_1 Z_2^2 \qquad U_1 = X_2 Z_1^2 \qquad S_0 = Y_1 Z_2^3 \qquad S_1^1 = Y_2 Z_1^3$$

$$W = U_0 + U_1 \qquad R = S_0 + S_1 \qquad L = Z_1 W_i V = RX_2 + LY_2$$

$$Z_3 = LZ_2 \qquad T = R + Z_3 \qquad X_3 = aZ_3^3 + TR + W^3$$

$$Y_3 = TX_3 + VL^2$$

$2P_1 = P_3$

$Z_3 = X_1 Z_1^2$

$X_3 = (X_1 + cZ_1^2)^4$

$U = Z_3 + X_1^2 + Y_1 Z_1$

$Y_3 = X_1^4 Z_3 + VX_3$

$C = b^{2m-2} (\mathrm{mod}\, f(x),2)$ $\lambda = \dfrac{y_1 + y_2}{x_1 + x_2} (mf(x),2)$ $\qquad \lambda = \dfrac{y_2 - y_1}{x_2 + x_1} (mp)$

$$\lambda = x_1 + \frac{y_1}{x_1} (mf(x),2) \qquad (2)$$

$$\frac{3x_1^2 + a}{2y_1} = \lambda$$

$$(x_1 + x_2) \,\mathrm{mod}(f(x),2) \qquad (\mathrm{x}_3, \mathrm{y}_3) \qquad (3)$$

$$(x_1 + x_2) x^{-1} \,\mathrm{mod}(f(x),2) = 1$$

$$x_1 x^{-1} \equiv 1(\mathrm{mod}\, f(x), 2) \quad (4)$$

Рішення (4) вимагає значних ресурсів, алгоритму Евкліда.

m ≥160

У проективних координатах немає розподілу по суті.

$$F(2^m)F(2^m)F(2^m)$$

Завжди буде однозначність відображення з афінних координат у проективні і навпаки.

Тест Ламана

P, RSA, Д - Н : ?

$$P_C \le 2^{-t} \qquad (a, m) = 1 \quad (5)$$

Імовірність, що число просте не перевищує 2^{-t}.

Числа Кармайкла ("брудні поросята")

561, 3, 11, 17

Вони проходять цей тест. Чим більше t, тим менше імовірність проходження в тесті.

Тест Соловея – Штрассена.

Базується на t – іспитах, генерується t – раз.

1) (a_i, m), причому $1 \le a_i \le m-1$, a_i генерується t -раз.

2) перевіряється НСД, $(a_i, m) \ne 1$, те число складене.

3) знаходиться символ Якобі

$$\frac{a}{m} \ne a_1^{\frac{m-1}{2}} (\mathrm{mod}\, m) \text{ - число складене} \quad (6)$$

$$\frac{a_m - 1}{2} = m - 1(-1)$$

P=7 1 2 4 1 2 4 1

a=3 i | 0 1 2 3 4 5 6 Справедливо (5).

ai | 1 3 2 6 4 5 1

Тест Рабінера - Міллера

Нехай m – непарне, просте, представимо:

$$m - 1 = 2^S t \quad (7)$$

m, s - не пара

$$a^t, a^{2t}, a^{4t}, ...a^{2^S t} \quad (9)$$

З обліком (7) випливає:

$$a^{2^S t} \equiv 1(\mathrm{mod}\, n) \quad (8)$$

У ряді (9) кожен попередній елемент є корінь з наступного елемента.

a^i - елементи поля, $a^{2^S t} = 1$, $\sqrt{1} = \pm 1$, то ряд (9) складається з одиниць, перед якими може випливати -1, чи

$$a^t \equiv 1(\mathrm{mod}\, m) \quad (10)$$

чи для всіх $0 \le j \le s$ $\quad a^{2^{jt}} \equiv -1(\mathrm{mod}\, m)$

Число m, що задовольняє хоча б одній умові, називається сильним псевдопростим у змісті Рабінера – Міллера.

Якщо проводити t– іспитів, то імовірність того, що в кожнім іспиті не буде виявлене просте число не перевищує ¼.

На t – іспитах

$$P_C \le \left(\frac{1}{4}\right)^t = 2^{-2t} \quad (11)$$

Порівнюючи з (5) бачимо, що збіжність тесту Рабінера – Міллера набагато вище.

Алгоритм перевірки

1. $1 \le a_i < m-1$
2. НСД $(a_i, m) \ne 1$ m – складене
3. $y_0 = a_i^t (\mathrm{mod}\, m)$
4. якщо $y_0 = t(\mathrm{mod}\, m)$ m – можливо просте
5. $y_j = y_{j-1}^2 (\mathrm{mod}\, m)$ доти поки $y_j = \pm 1(\mathrm{mod}\, m)$
6. якщо $y_j = 1(\mathrm{mod}\, m)$, те m – складене

якщо $y_j = -1(\mathrm{mod}\, m)$, m – можливо просте

$$P_C^1 \le 1/4$$

Проводимо t1 – експериментів, після цього підтверджуємо (11).

$$P_C \le 2^{-2t_1}$$

1. Знайти a_i, $\mathrm{GF}(2^4)$, $\mathrm{f(x)} = \mathrm{x}^4 + x + 1$, $\mathrm{m} = 4$
2. Добуток і сума

$$a_1 = 1101 \qquad \mathrm{a}_2 = 1001$$

3. $a_i \in GF(2^4)$ $\quad \mathrm{x} = \alpha(0001)(\mathrm{f(x)} = \mathrm{x}^4 + x + 1$

$$x^0 = \alpha^0(mf(x)) \qquad x^1, x^2$$

Лекція 11

Принципи реалізації спрямованого шифрування

1. Спрямоване шифрування в кільцях і полях.
2. Методи спрямованого шифрування в групах точок ЕК.
3. Обговорення результатів.

Сутність спрямованого шифрування в RSA - алгоритмі.

$$C_i = M_i^{E_K} (\mathrm{mod}\, N_j) \quad (1)$$

$$M_i = C_i^{D_K} (\mathrm{mod}\, N_j) \quad (2)$$

$$\begin{cases} E_K - \text{открытый ключ} \\ \mathrm{D_K} - \text{закрытый ключ} \end{cases}$$

$$E_K D_K \equiv 1(\mathrm{mod}\,\varphi(N_j)) \text{ - випадкова пара}$$

Якщо пари $E_K D_K$ генерується k– им користувачем, то він може записати E_K на носій у захищеному виді і зберегти його в таємниці. E_K перетвориться в сертифікат і розсилається усім внутрішнім користувачам. У цьому випадку всі користувачі володіють E_K и N_j. Можуть здійснювати спрямоване шифрування за правилом (1). Розшифрувати C_i - криптограму може тільки k - ий користувач, що володіє D_K - ключем. Такий несиметричний шифр називається спрямованим шифром.

Недоліки RSA спрямованого шифру

Доказова стійкість, її доказ зводиться до факторизації N_j. Розвиток математичних методів і криптоперетворень приводить до зменшення складності факторизації.

Сутність перетворення Ель – Гамаля

1 етап: являє собою реалізацію розподілу ключів по відкритих каналах зв'язку. Усі користувачі одержують загальносистемні параметри (P_j, Θ_ν), де P – просте, Θ - первісний елемент (у всіх користувачів вони однакові). Кожен користувач генерує особистий ключ X_A, X_B, що являє собою випадкову послідовність (x не менше 160 біт). Потім x – компоненти з'являються особистими ключами і зберігаються в таємниці. Після цього кожен користувач обчислює відкриті ключі. Потім відкриті ключі поширюються в мережі з забезпеченням цілісності і дійсності.

(P_j, Θ_ν)

$$X_A \quad {}^{\mathrm{A}_0} \qquad\qquad {}_0{}^{\mathrm{B}} X_A$$

$$Y_A = \Theta_\nu^{X_A} (\mathrm{mod}\, P_j) \qquad Y_B = \Theta_\nu^{X_B} (\mathrm{mod}\, P_j) \tag{3}$$

2 етап: ключ спрямованого шифрування

$$K_{AB} = Y_B^K (\mathrm{mod}\, P_j) \tag{4}$$

К – сеансовий ключ, випадкове число.

(k,p-1) = 1

Нехай необхідно зашифрувати M_i - ий блок. Далі обчислюються компоненти:

$$C_1 = \Theta_\nu^K (\mathrm{mod}\, p) \tag{5}$$

і сеансовий відкритий ключ, після обчислюється відкрита криптограма:

$$C_2 = K_{AB} * M_i (\mathrm{mod}\, p_j) \tag{6}$$

Передачі підлягає $\{C_1, C_2\}$ щораз. Операція групова.

Розшифрування

Одержувач B на початку підносить $C_1^{X_B} (\mathrm{mod}\, P_i) = K_{BA}$ до X_B степеня.

$$K_{AB} = (\Theta_v^{X_B})^K (\mathrm{mod}\, P_j) = \Theta_v^{X_{BK}} (\mathrm{mod}\, P_j) \quad (7)$$

$$K_{AB} = (\Theta_v^{X_B})^K (\mathrm{mod}\, P_j) = \Theta_v^{K_{XB}} (\mathrm{mod}\, P_j) \quad (8)$$

(7) = (8)

Отже, можна розшифрувати 32.

$$M_i = C_2 \otimes K_{AB} (\mathrm{mod}\, P_j) \quad (9)$$

* - множення

(- зворотне, тобто розподіл

Підсумок:

1. має більш високу стійкість, чим RSA, для її розкриття необхідно визначити X_A и K і така можливість є. Перебування X_A - задача дискретного логарифма.
2. Компрометація X_A ще не приводить до повної компрометації всієї криптограми.
3. Завдання.

Показати, що якщо 31 використовується для декількох блоків, то така криптограма зламується за поліноміальний час (не вище чим з поліноміальною складністю).

На рис.10.1 приведена спрощена схема керування шифрування в групах точок ЕК.

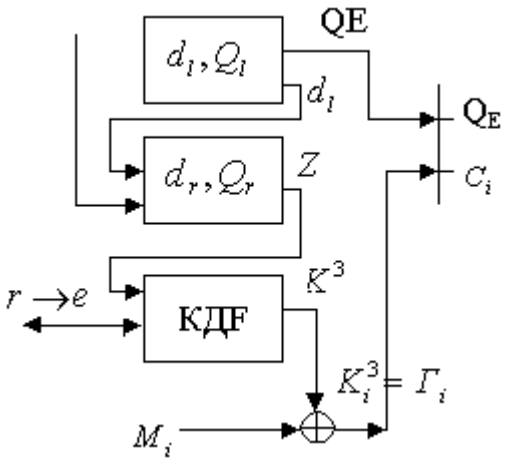


рис.10.1- Спрямоване зашифрування

$$C_i = M_i \oplus K_i^3 \quad (10)$$

Зашифрування

При розгляді структури зашифрування будемо думати, що l і r відомо користувачу (a, b, f(x),q, u, g, nc) загальносистемні параметри. Будемо думати, що l і r здійснили 1 етап розподілу ключів за схемою Діфі – Хелмана. $e \to (d_e, Q_e)$, $r \to (d_r, Q_r)$. Для зашифрування використовується Q_r - відкритий ключ одержувача, відповідно до методу Ель – Гамаля генерується d_e, Q_e - сеансовий ключ, причому d_e використовується тільки для зашифрування, а Q_e передається одержувачу разом із криптограмою. На першому кроці обчислюють загальний секрет :

$$Z = d_l, Q_l (\mathrm{mod}\, f(x), 2) \quad (11)$$

Z перетворюється в бітовий рядок (Z = Xz – наприклад). І далі цей бітовий рядок надходить у блок КД формування ключової послідовності Γ_i чи зашифрування. Z є вихідним ключем. На виході КД формуються $K_i^3 = \Gamma_i$ зашифрування і повідомлення зашифровується. Ключ зашифрування в КД формується на основі ключа Z, додаткових даних Д, що користувач вибирає сам і за рахунок хешування інформації.

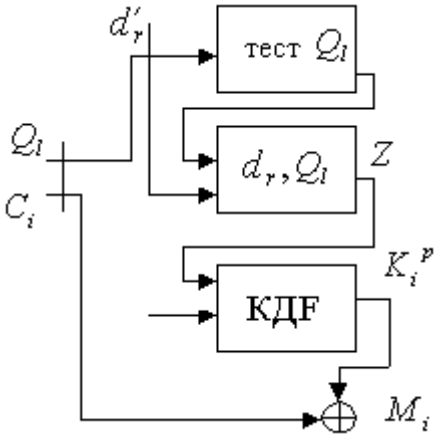


рис.10.2 – Спрямоване розшифрування

$$M_i = C_i \oplus K_i^p \quad (12)$$

При цьому h_i блоки формуються як :

$$h_i = H(Z \,\|\, счет\ Д) \quad (13)$$

Ні – елемент ключа зашифрування

$K_i^3 = \Gamma_i - (h_1, h_2, ...h_n)$ - випадкова послідовність.

Розшифрування

Тестуємо Q_e - перевіряється цілісність Q_e, потім обчислюється загальний секрет Z з використанням d_e, Q_e. КД формує Γ_i розшифрування по методу (13), далі здійснюється потокове розшифрування.

Висновки:

У такий спосіб застосування протоколу Діфі – Хелмана на ЕК разом із симетричним зашифруванням / розшифруванням дозволяє з однієї сторони здійснити спрямоване зашифрування, з іншої сторони дозволяє здійснити симетричне шифрування. По суті нам потрібно виконати обчислення Q_e и Z тільки один раз на початку сеансу. Реалізуються більш високі швидкості шифрування. Стійкість базується на рішенні дискретного логарифма в групах точок ЕК.

Лекція №12

Теорія автентичності

Вступ. Модель погроз

1. Основні поняття і визначення.
2. Модель погроз.
3. Вступ у теорію автентичності професора Симонсона.

Основні поняття і визначення

Цілісність інформації і ресурсів – це властивість захищеності інформації від випадкової чи навмисної її модифікації яка забезпечується за рахунок застосування криптографічних методів захисту інформації.

Спостережність – є властивість захищеності інформації і ресурсів (комп'ютерні мережі, АСУ і т.д.), що забезпечує реєстрацію і спостереження за діями об'єктів процесу й автентифікацію всіх об'єктів процесу, відстеження небезпечних дій, попередження обмеження чи користувачів процесів, насамперед за рахунок криптографічного захисту інформації.

Ідентифікація – це процедура присвоєння об'єктам, суб'єктам, процесам унікального імені чи коду, наявність якого дозволяє однозначно виділити цей об'єкт чи процес серед іншого.

Автентифікація користувача – це процедура встановлення дійсності об'єкта чи суб'єкта, що звертається до інформації, що захищається, чи ресурсам.

Автентифікація мережі – це процедура встановлення дійсності чи мережі інформаційної технології, до яких отриманий доступ даним чи об'єктам суб'єктам.

Автентифікація інформації – це процедура цілісності цієї інформації, якщо вона в плині деякого часу Δt знаходився поза контролем власника і підтвердження авторства цієї інформації.

Автентифікація повідомлень - це процедура цілісності і дійсності повідомлення, отриманого від визначеного об'єкта.

Причетність до створеної інформації – це процедура підтвердження, у тому числі і юридично, того факту, що інформація створена чи відправлена, цим чи об'єктом суб'єктом.

Невідмовність одержувача - це процедура підтвердження, у тому числі і юридично, факту прийому й обробки, чи об'єктом суб'єктом, конкретної інформації.

Автентифікація здійснюється за рахунок застосування систем паролювання цифрових підписів і кодів автентифікації системи.

Модель погроз

На рис.11.1 представлена спрощена схема моделі взаємної недовіри і взаємного захисту:

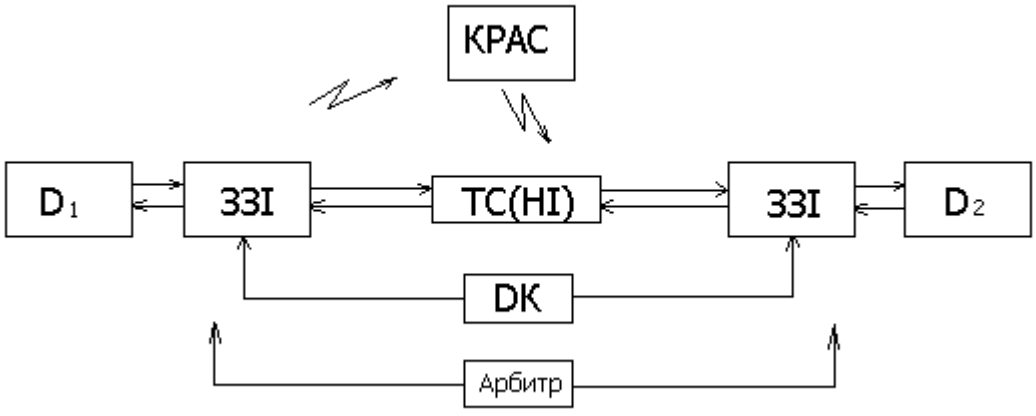


Рис.14.1

ТС (НІ) – телекомунікаційна мережа (носій інформації);

ЗЗ – захист захисту інформації;

КРАС – криптоаналітик (зловмисник);
ДК – джерело ключів;
Д – джерело інформації.
Виділимо 4 суб'єкта:
- D_1;
- зловмисник (КРАС);
- арбітр;
- D_2.

Вони не довіряють один одному.

Погроза D_1*:*

1) D_1 формує повідомлення M_i, а потім відмовляється від факту передачі її в мережу.

2) Джерело D_1 затверджує, те він сформував деяку інформацію M_i і можливо він неї передав у мережу, а насправді він її не формував і не посилав.

3) D_1 затверджує, що він сформував і передав інформацію M_i у визначений час, хоча насправді він неї сформував і передав іншим часом.

4) D_1 формує і передає інформацію M_i', а потім затверджує що була передана інформація M_i.

Погроза D_2*:*

1) D_2 формує деяку M_i' інформацію, а потім D_2 затверджує, що він неї одержав від D_1.

2) D_2 одержує M_i інформацію від D_1, а потім модифікує її в M_i', а потім затверджує, що він одержав інформацію M_i'.

3) D_2 затверджує, що він одержав інформацію M_i в момент часу t_i, а насправді він одержав інформацію під час t_j.

Погроза КРАС:

1) Імітація помилкового повідомлення M_i, КРАС у момент часу, коли D_1 пасивний, він створює помилкову M_i інформацію і передає її D_2 (чи D_1).
2) Модифікація вірної інформації M_i, у випадку якщо D_1 передає D_2, деяку інформацію M_i, КРАС модифікує інформацію M_i в M_i' і передає її D_2.
3) Нав'язування рішення створеної інформації, тобто D_1 в будь-який момент часу t_j передає її ще раз D_2, коли D_1 пасивний.
4) Передача помилкових команд керування мережними службами, помилкові команди керування ключами.

Погроза арбітра:

Арбітра можна вважати зловмисником і не довіряти йому, від нього потрібно захищатися.

Задача систем забезпечення цілісності і спостерігаемості інформації – мінімізувати втрати при спектрі безлічі погроз.

Вступ у теорію автентичності професора Симонсона

У 70-і роки вперше була опублікована теорія оцінок автентичності, тобто теорія Симонсона.

Сутність теорії Симонсона:

У теорії Симонсона покладається, що два користувачі D_1 і D_2 взаємодіють між собою по відкритій телекомунікаційній системі (ТС) і для обміну між ними виділяється одноразовий ключ автентифікації.

Будемо вважати, що простір повідомлень M_i може бути сформоване з n_{M_i} повідомлень.

ЗЗ – захищає інформацію M_i, він формує:

$C_i = F^+(M_i, K_j^+, \Pr);$ (1)

C_i - передається по ТС, а потім ЗЗ відновлює інформацію:

$M_i' = F^-(C_i', K_j^-, \Pr);$ (2)

Будемо думати, що джерело криптограм формує n_{C_i} - криптограм. Якщо КРАС сформує безліч криптограм n_{C_i} і він одну передав, то він може нав'язати обман.

$$P_{об} = \frac{n_M}{n_C},$$ (3)

де $P_{об}$ - імовірність обману.

Якщо $n_M = n_C$, то імовірність нав'язування повідомлення дорівнює 1.

Наша задача зменшити $P_{об}$, для цього необхідно збільшити простір криптограм:

$n_M < n_C;$ (4)

Для створення безумовно стійкою системи $n_C \to \infty$, тоді час передачі інформації буде ∞, тому ніколи не можна створити криптографічний захист де $P_{об} = 0$, тому необхідно якнайбільше зменшити $P_{об}$.

Лекція 13

Методи автентифікації

Навчальні питання

1. Основні положення теорії.
2. Класифікація методів автентифікації.

1. Основні положення теорії.

Модель Симонсона.

$$P_{об} = \frac{n_м}{n_c},$$ (1)

де $n_м$ - розмір джерела повідомлення, n_c - розмір криптограми. Якщо $n_м = n_c$, то в системі може бути нав'язане повідомлення випадкового змісту. КРА в моделі рис.14.1 може реалізувати наступні загрози:

1. Імітація. P_u - ймовірність імітації.
2. Підміна. P_n - ймовірність підміни.
3. $P_\sum$ - ймовірність всіх останніх загроз.

Треба при проектуванні та оцінці автентичності визначити, яка загроза є найбільш небезпечною.

У своїй теорії Симонсон здійснює оцінку по одній найбільш небезпечній загрозі.

$$P_{обм} = \max(P_u, P_n, P_{pn}, P_\sum)$$ (2)

Він визначив $P_{обм}$ як максимальну загрозу із всієї множини загроз.

Покладемо, що джерело $D1$ разом з ЗЗІ формують криптограму C_i та відомий апріорний ряд $P(C_i)$ для $i = \overline{1, n_c}$. При відомому $P(C_i)$ можна знайти ентропію джерела повідомлення криптограм $D1$:

$$H(C) = -\sum_{i=1}^{n} P(C_i) \log P(C_i)$$ (3)

КРА, перехоплюючи криптограми, намагається визначити ключ автентифікації, який використовується для забезпечення цілісності та достовірності. Незнання КРА відносно

ключа або надмірності, внесеної в криптограму, можна записати як умовну ентропію, що ключ K_j використовується для криптограми C_i:

$P(C_i/K_j)$ - вважаємо відомою,

$$H(C/K) = -\sum_i \sum_j P(C_i, K_j) \log_2 P(C_i/K_j) = -\sum_{i=1} \sum_{j=1} P(K_j) P(C_i/K_j) \log_2 P(C_i/K_j)$$

(4)

Визначимо, яку кількість інформації ΔI отримав КРА при переході від $H(C)$ до $H(C_i/K_j)$:

$\Delta I(C,K) = H(C) - H(C/K)$.

Сімонсон показавши, що для моделі (2), коли вибирається тільки одна загроза, ймовірність обдурю може бути обчислена по формулі:

$$\log_2 P_{обм} \geq -\Delta I(C,K) \qquad (5)$$

Знайдемо із (5) $P_{обм}$:

$$\mathrm{P}_{\text{обм}} \geq 2^{-\Delta I(C,K)} \qquad (6)$$

Вираз (6) у теорії Сімонсона визначає межу ймовірностей обману в системі.

Розглянемо (6):

1. Криптосистеми, у яких досягається рівність (6), називаються системами з найкращим способом автентичності (повністю автентичні).
2. Для зменшення ймовірності обману необхідно збільшувати $\Delta I(C,K)$, тобто кількість інформації, що міститься в криптограмі про ключ автентифікації.
3. Для забезпечення цілісності та достовірності необхідно вводити додатковий ключ автентифікації K_a. Таким чином у нашій системі з'явиться 2 ключі – ключ шифрування $K_ш$ та ключ автентифікації K_a.

$$P_{обм} \geq 2^{-l_u} \qquad (8)$$

де l_u - довжина імітовставки.

Розглянемо (1) та (8). Нехай довжина повідомлення буде $l_м$ бітів. Довжина контрольної суми l_u. Тоді довжина криптограми:

$$l_c = l_м + l_u \qquad (9)$$

Тоді для двоїчного алфавіту

$$n_м = 2^{l_м};\ n_c = 2^{l_c} = 2^{l_м + l_u} \qquad (10)$$

Підставимо (10) у (1):

$$P_{обм} \geq \frac{2^{l_m}}{2^{l_m + l_c}} = 2^{-l_u} \qquad (11)$$

(11) співпадає з (8).

2. Класифікація методів автентифікації.

Всі методи автентифікації можна розділити на 2 класи: ті, що реалізуються збитковістю, і ті, які без збитковості.

Теорема 15.1.

Поточне шифрування є необхідною, але не достатньою умовою забезпечення цілісності та достовірності переданої інформації.

Доведення. Розглянемо поточне m-ічне шифрування. Нехай M_i є повідомлення криптограми. Γ_i - функція зашифрування.

$$\Gamma_i = \varphi(K_j^u), \qquad (15)$$

де K_j^u - початковий j- тий ключ. Тоді

$$C_i = M_i \oplus \Gamma_i . \qquad (13)$$

Покладемо, що КРА може перехватити тільки C_i та зможе сформувати послідовність R_i (яку-небудь). Тоді він формує $C_i' = C_i \oplus R_i = M_i \oplus \Gamma_i \oplus R_i$. Будемо вважати, що ЗЗУ має синхронізацію по і. Тоді відновленням повідомлення отримаємо: $M_i' = C_i' \oplus \Gamma_i = M_i \oplus \Gamma_i \oplus R_i \oplus \Gamma_i = M_i \oplus R_i$. Таким чином, нав'язати хибне повідомлення неможливо. Теорему доведено.

У більшості відкритих додатків джерело $D1$ не довіряє $D2$. Більш того, обоє прагнуть захисту від арбітражу. Це може бути досягнуто, якщо в системі використовується несиметрична криптографія.

Лекція 14

Методи забезпечення цілісності та достовірності у класі симетричних шифрів.

Навчальні питання:

1. Методи автентифікації в симетричних потокових системах.
2. Методи автентифікації в блокових симетричних системах.

1. Методи автентифікації в симетричних потокових системах.

Теорема 14.1.

Використання потокового шифрування та групових кодів, що знаходять та виправляють помилки, є необхідною, але не достатньою умовою забезпечення цілісності та достовірності захищаємої інформації.

Доведення. Нехай М – інформація. M_i – блоки інформації М. При груповому кодуванні обчислюються контрольні символи як

$$KC = \psi(M_i) \qquad (1)$$

Після цього в систематичному груповому коді шкірному блокові додається КС: $M_i ; KC = M_i'$. На прийомній стороні в декодері на основі КС знаходяться та виправляються помилки, якщо їх не більше, ніж виправна здібність коду. Для захисту M_i використовується поточне шифрування:

$$C_i = M_i' \oplus \Gamma_i \qquad (2)$$

Групові коди володіють властивістю, що операція $\oplus$ є дозволеною комбінацією цього ж коду, тобто властивість замкнутості:

$M_i' \oplus M_v' = M_\zeta'$.

Якщо КРА може нав'язати хибну інформацію методом модифікації, додавши $C_i \oplus M_v$, то декодер прийме M_ζ і цієї модифікації не виявить її.

Теорему доведено.

Висновок: у відповідності з Т.14.1 у поточних системах, які використовують групові коди, може нав'язуватися інформація як випадкового так і визначеного змісту.

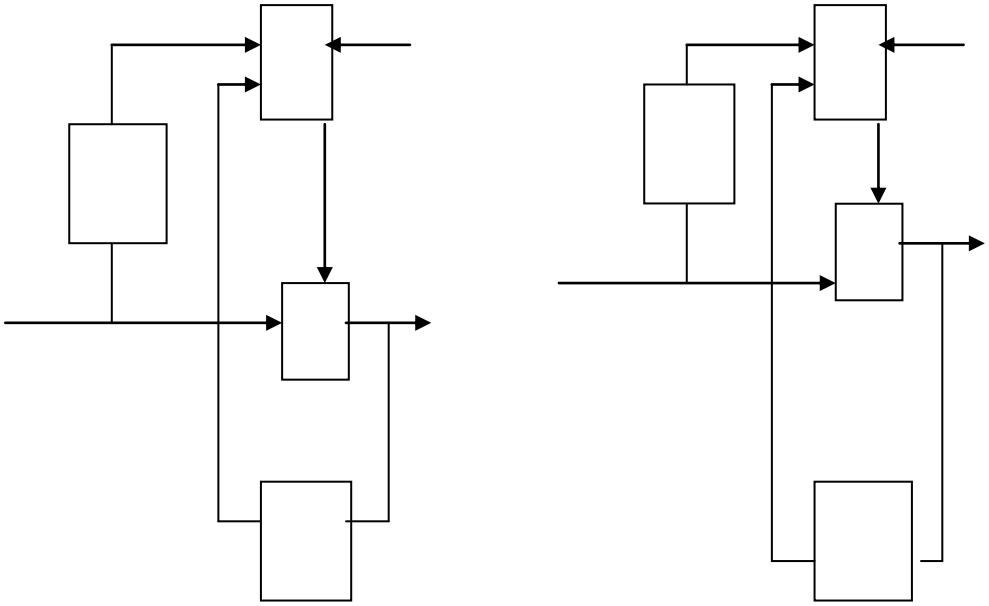
Теорема 14.2

Необхідною і достатньою умовою забезпечення цілісності та достовірності в системах потокового шифрування є:

- використання потокового шифрування;
- використання групових кодів, виявлення помилок;
- формування Г шифруючої з використанням раніше переданих символів криптограми або відкритої інформації.

Рис.14.1. – 14.2

Роздивимося на рис. 14.1, 14.2



$C_i = M_i \oplus \Gamma_i^*$ (4)

де $\Gamma_i^* = \Gamma_i \oplus (\Pi(\sum C_{i-\xi} \vee (\wedge)\Pi(\sum M_{i-\xi}))$ (5)

у нашому випадку зашифрування $C_i = M_i \oplus \Gamma_i \oplus (\oplus\sum C_{i-\xi} \vee (\wedge) \oplus \sum M_{i-\xi})$ (6)

розшифрування

$$M_i^{'} = C_i^{'} \oplus \Gamma_j^{*'} = M_i^{'} \oplus \Gamma_i^{'} \oplus (\sum C'_{i-\xi} \vee \sum M'_{i-\xi}) \oplus \Gamma_i \oplus (\sum C_{i-\xi} \vee \sum M_{i-\xi}) =$$

$$= M_i^{'} \oplus (\Gamma_i^{'} \oplus \Gamma_i) \oplus (\sum C'_{i-\xi} \vee \sum M'_{i-\xi}) \oplus (\sum C_{i-\xi} \vee \sum M_{i-\xi})$$

$\Gamma_i^{'}$ - Γ, яку сформоване на приймачі.

Якщо $\Gamma_i^{'} = \Gamma_i$, тобто сформувати правильно, то $\Gamma_i^{'} = \Gamma_i = 0$. І вирази з сумами відповідно $=0 \Rightarrow M_i^{'} = M_i$ - це значити інформацію прийняли правильно.

Якщо $\Gamma_i^{'} \neq \Gamma_i$, то $M_i^{'} \neq M_i$ - не правильно.

Наприклад, розшифрувати з помилкою $M_i^{'}$ затримується і приймають доля у формуванні Γ_i. Це приводити до неправильного розшифруванню.

Кодові комбінації автоматично виявив факт появи помилки і автоматично відмовляється від цієї інформації $M_i^{'} \Rightarrow$ нав'язування не відбувається.

2. Методи автентифікації в блокових симетричних шифрах.

Здійснюється на основі обчислення для шкірного блоку криптографічної контрольної суми. КАС

$$Імст = \varphi(M, K_ш, K_a, \Pr) \qquad (7)$$

Імітовставка формується як з використанням $К_ш$, так і з використанням $К_а$. Алгоритм обчислення КАС, показане на рис. 14.3.

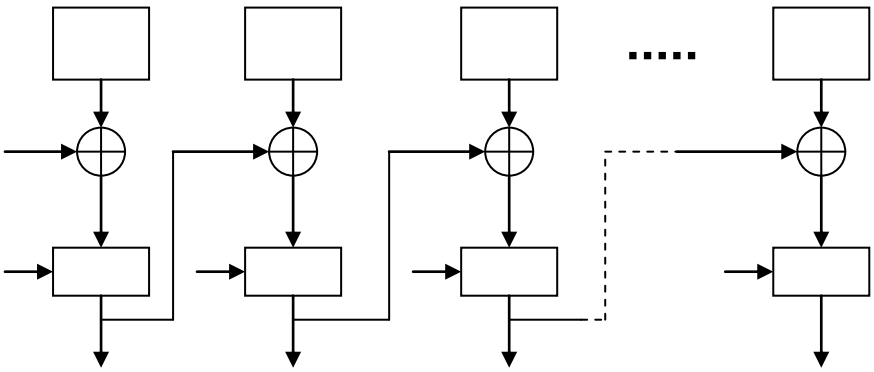


Рис.14.3

Імітовставка залежить від усіх блоків даних, смороду беруть доля в її формуванні (це видно з малюнку 14.3).

Таким чином цілісність та достовірність можуть бути забезпечені тільки за рахунок введення збитковості. Для потокового шифрування – у вигляді контрольних кодових комбінацій, а для блокових – у вигляді імітовставки.

Перевірка цілісності:

Прийняте повідомлення разом з імітовставкою перетворюється так:

1. спочатку з M' обчислюється $Імст'$, використовуючи (7).
2. береться $Імст*$ і порівнюється з $Імст'$ обчисленою, якщо $Імст* = Імст'$, то повідомлення цілісне та достовірне. Ймовірність обману оцінюється як:

$$P_{обм} \geq 2^{-l_u}.$$

Лекція 15

Поняття та властивості цифрового підпису

Навчальні питання:

1. Поняття ЦП;
2. Класифікація та вимоги до ЦП;
3. Підписи в класі перетворень Ель - Гамаля та RSA і проблемні питання;

1. Поняття ЦП

Основним недоліком симетричних перетворень є те, що в них не можна реалізувати модель взаємної недовіри.

Використання систем з відкритими ключами (перетворення в полях, кільцях ЕК) дозволяє реалізувати модель взаємної недовіри та взаємного захисту.

Підпис, у тому числі і цифрова, повинна володіти наступними властивостями:

- автентичність підпису;
- мала ймовірність підробки підпису під документи;
- мала ймовірність не виявлення зміни змісту документа;
- неможливість “приклеювання” до нового документу підпису зі старого документу;
- незаперечність підпису;
- упізнаваємість підпису;

Поняття ЦП: під ЦП розуміється деякий числовий еквівалент звичайного підпису (штампу, печатки і т.п.), наявність яких дозволяє встановити цілісність та достовірності документу. Підробити цей підпис можливо лише з ймовірністю, що не перевищує $P_{обм} \leq P_{доп}$.

Під ЦП розуміється криптографічна контрольна сума, що обчислюється з використанням несиметричної криптографії. Під відкритим підписом (ВП) розуміється сукупність відкритих даних, що характеризуються:

1. захищаємою інформацією;
2. взаємодією абонентів;
3. година створення та година життя інформації;
4. інше.

$$ОП = (H(M), I_0, I_n, t_c, \text{Pr}) \quad (3)$$

де $H(M)$ - зжате перетворення інформації (хеш - функція), I_0 - ідентифікатор відправника, t_c - час життя та створення, I_n - ідентифікатор одержувача.

На основі ВП формується ЦП:

$$ЦП = F^{пр.пр}(M, A_n, K^{пр.пр}, \text{Pr}) \quad (4)$$

де A_n - данні користувачів, M - данні, $K^{пр.пр}$ - ключ прямого перетворення.

Вимоги до ЦП:

1. складність обчислення ЦП повинна бути не вища поліноміальної;
2. алгоритм обчислення криптоперетворення ЦП (4) винний бути загальнодоступним;
3. складність знаходження $K^{пр.пр}$ повинна бути не нижча, ніж експоненціальна;
4. ЦП винний бути дуже чутливий до зміни навіть одного біту в повідомленні, ключі та параметрах.
5. ЦП повинний дозволяти проводити перевірку цілісності та достовірності повідомлення, тобто з високою ймовірністю знаходити цілісність та достовірність.

$P_{доп} = -10^{-36}$.

6. ЦП повинний бути захищеним від будь-якого класу криптоаналітичних атак (складність яких менше, ніж атака груба сила).

2. Класифікація та вимоги до ЦП

Класифікація на основі криптоперетворення в полях, кільцях та групах точок еліптичних кривих. На теперішній час в частині додатків розроблений ЦП, який використовується в криптографічних протоколах для реалізації:

1. для безпечних електронних виборів;
2. сумісний електронний підпис контрактів;
3. груповий підпис з забезпеченням анонімності;
4. довірений підпис;
5. незаперечний підпис;
6. сліпий підпис;
7. підпис типу - передача, що забувається;
8. виробка загального секрету;

3. Підписи в класі перетворень Ель - Гамаля та RSA і проблемні питання

У RSA системі в якості загальносистемних параметрів: $N_j = P_j \cdot Q_j$. (5)

У ористувача N_j повинне бути різним.

$$ЦП = ОП^{E_k} (\text{mod}\, N_j) \quad (6)$$

де E_k - ключ ЦП.

$$E_k \cdot D_k \equiv 1 (\text{mod}\, \varphi(N_j)) \quad (7)$$

Перевірка ЦП: при перевірці користувач, що володіє відкритим ключем D_k, знаходить ОП:

$$ОП' = ЦП^{D_k} (\text{mod}\, N_j) \quad (8)$$

Після цього перевіряючий встановлює всю інформацію через хеш - функцію:

$$ОП' = (H(M), I_0, I_n, t_c, \text{Pr}) \quad (9)$$

На основі аналізу складових ЦП знаходиться цілісність та достовірність, у тому числі підписана інформація M має вид:

$$[M, ЦП] \quad (10)$$

Якщо порівняння (10) виконується, то повідомлення вважається цілісним та достовірним з деякою ймовірністю.

Стійкість залежить від факторизації $N_j = P_j \cdot Q_j$. (11)

У класі перетворень Ель - Гамаля система ЦП здійснюється за два етапи:

1. здійснюється генерація та розподілення ключів, тобто кожен користувач, генерує собі ключ, зберігає його в собі в таємниці, а відкритий ключ обчислює як:

$$Y_A = \theta_v^{x_F} (\mathrm{mod}\, P) \tag{12}$$

Відкритий ключ розповсюджує всім кореспондентам системи.

2. на цьому етапі Ель - Гамаль запропонував сформувати підпис як дві компоненти ЦП: $\{r, s\}$.

Ці компоненти формуються на основі розв'язку класичного порівняння Ель - Гамаля:

$$\theta^{H(M)} \equiv Y^r \cdot r^s (\mathrm{mod}\, P) \tag{13}$$

де θ_v - первісний елемент у полі, $H(M)$ - хеш - функція, Y - відкритий ключ.

$$h = H(M) \tag{14}$$

$$r = \theta^k (\mathrm{mod}\, P) \tag{15}$$

Підставимо (12) та (15) у (13):

$$\theta^h \equiv \theta^{x_A \cdot r} \cdot \theta^{k \cdot s} (\mathrm{mod}\, P) \tag{16}$$

$$\theta^h \equiv \theta^{x_A \cdot r + k \cdot s} (\mathrm{mod}\, P) \tag{17}$$

$$h \equiv (x_A r + ks) \bmod (P-1) \tag{18}$$

(18) є фундаментальним виразом, бо дозволяє обчислити другу компоненту ЦП, а саме s:

$$s = \frac{h - x_A r}{k} (\mathrm{mod}(P-1))$$

$$s = (h - x_A r) k^{-1} (\mathrm{mod}(P-1)) \tag{19}$$

Перевірка: здійснюється всіма користувачами, які володіють відкритим ключем та загальносистемними параметрами. Здійснюється на основі перевірки порівняння (13).

Стійкість перетворення визначається складністю розв'язку порівняння (12).

Методи та алгоритми формування псевдовипадкових послідовностей з m-ічною основою

1. Вимоги, пропоновані до псевдовипадковим послідовностей.
2. Лінійна рекурентна послідовність з максимальним періодом.
3. Псевдовипадкова послідовність на базі многомодульних перетворень.

З класичної теорії стійкості й автентичності випливає, що передбачуваний рівень стійкості, що розраховується, і автентичності виходить у тому випадку, якщо загальносистемні параметри і ключ породжуються випадково, рівноймовірно і незалежно. Випадкові компоненти повинні формуватися на основі випадкових чи псевдовипадкових процесів. У ряді додатків необхідно застосовувати псевдовипадкові послідовності з необхідними властивостями.

Основні властивості:

1. Основа алфавіту - m.
2. Період повторення - L.
3. Відновлюваність.
4. Псевдовипадкові властивості.
5. Структурні властивості послідовностей.

На теперіщній час відомий ряд алгоритмів і засобів формування псевдовипадкових послідовностей. Основною їхньою особливістю є те, що вони будуються для 2-ічної основи (m=2). Відомий клас m – ічних послідовностей, володіє незадовільними структурними властивостями в змісті значної залежності появи символів послідовності. Для визначення закону формування таких псевдовипадкових послідовностей необхідно і досить одержати безпомилково 2l – символів, де l – база лінійного рекурентного регістра, тому дуже важливої і необхідний є задача розробки математичних алгоритмів і засобів побудови псевдовипадкової послідовності (ПСП) із заданими необхідними властивостями і підставою алфавіту m. До найбільш перспективному, на наш погляд, класу таких перетворень відноситься многомодульне перетворення.

Лінійні рекурентні послідовності з максимальним періодом

Для формування ЛРП максимального періоду застосовуються ЛРР (лінійний рекурентний регістр). Робота ЛРР по формуванню ЛРПМП цілком визначається багаточленом:

$$f(x) = A_0 X^2 + A_1 X^{n-1} + ... + A_{n-1} X + A_n \qquad (1)$$

A_i - коефіцієнти багаточлена над GF(q).

Нехай необхідно побудувати ЛРР, що виробляє двійкову ЛРПМП довжиною $2^n - 1$, робота якого визначається (1).

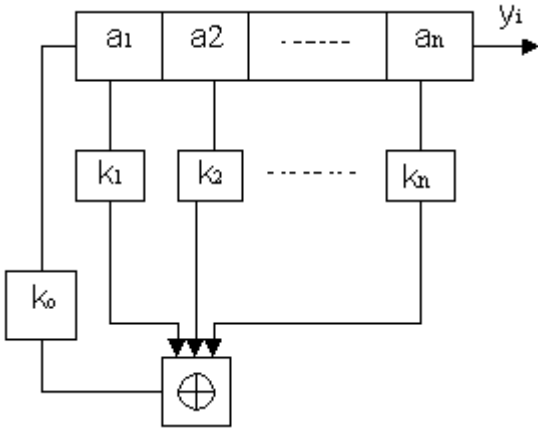


Рис.16.1 - Структурна схема цього регістра

$a_1, a_2, ...a_n$ - визначає поточне (початкове) стан.

$k_0, k_1, k_2, ...k_n$ - визначає необхідні зворотні зв'язки.

При подачі на ЛРР такту частоти регістр входить у робочий стан. На кожному і - тому такті вміст останнього регістру a_n зчитується на вихід y_i, тим самим доповнюючи ЛРПМП наступним символом. У той же час значення всіх регістрів збільшується на відповідні коефіцієнти k і надходять на вхід загального суматора. Результат підсумовування збільшується на ko і надходить на вхід регістра. На цьому робота ЛРР на черговому такті завершується. Т.к. ЛРР має період $2^n - 1$, те після $2^n - 1$ тактів роботи регістр приймає вихідне значення.

У нашому випадку необхідно одержати двійкову послідовність, тому вектор a_1, a_n є двійковим а в суматорі є сума (mod 2). Для розкриття формування закону ЛРПМП необхідно перехопити 2l – символів безпомилково, тобто якщо l =257 то 2*257=514біт.

Розглянемо правила перетворення в поле Галуа:

$$a_i = (a_{i-1} + \Theta_\nu) \bmod(P)$$

$$b_i = a_i(\bmod(P_1, P_2, ...P_{n-1}, P_n, m)) \quad (2)$$

a_i, a_{i-1} - елементи формованої послідовності.

Θ_ν - первісний елемент полючи Галуа.

$P_1, ...P_n$ - проміжні модулі.

m – основа алфавіту.

У (2) повинне виконуватися умови:

$$P >> P_1 >> P_2 >> ...P_n >> m >> 2 \quad (3)$$

Pn- довільна основа алфавіту символів формованої послідовності. Застосування (2) дозволяє з однієї сторони істотно підвищити кодову стійкість, тобто стійкість проти визначення закону формування псевдовипадкової послідовності, з іншої сторони дозволяє будувати послідовність з необхідною підставою алфавіту. Було здійснено всебічне тестування формування послідовностей з використанням статичних тестів (використовуючи критерій Пірсона χ^2 , визначення Холмогорова). Дані дозволили сказати, що використовуючи вираження (2) можна будувати m- ічні ПСП якого завгодно великого періоду, при цьому

також теоретично обґрунтоване, що m - ічні символи формованої послідовності з'являються також порівняно ймовірно і незалежно.

Тестування джерел випадкових і ПС чисел на основі методики стандарту США FIPS-140-1

Стандарт FIPS-140-1 визначає 4 статичних тести на випадковість:

- монобітний
- блоковий
- тест серій
- тест довжин серій

Для них задаються границі для задовільних значень, статичних параметрів. Окремий бітовий рядок довжиною 20 000 бітів піддається кожному з 4 приведених тестів.

Монобітний тест

Суть тесту в підрахунку кількості 0 і 1 на відрізку послідовності визначеної довжини.

n_0 "0" $n = n_0 + n_1$

n_1 "1" $x_1 = \frac{(n_0 + n_1)^2}{n}$

Послідовність а довжиною n, параметр x, підкоряється закону розподілу χ^2 з одним ступенем волі і цей тест може застосовуватися за умови, що n >10, якщо послідовність випадкова, те:

$$9654 < n_0(n_1) < 10346$$

Блоковий тест (Покеру)

Нехай послідовність має довжину n, хочемо перевірити появи блоків довжиною m.

$$k = \left[\frac{n}{m}\right] \qquad k >> 5 * 2^m$$

Поділимо послідовність а, довжини n на k – неперекриваючих частин, підрахуємо частоту появи різних блоків довжиною m.

$$x_2 = \frac{2^m}{k}\sum_{i=1}^{2^m} n_i^2 - k \qquad (4)$$

x_2 підкорюються χ^2 с 2^m ступенями свободи.

Методика перевірки полягає в тім, що спочатку розраховується експериментальне значення, а потім розраховуються граничні, додаткові значення і хі порівнюється з х граничним, якщо $x_i > x_n$, те гіпотеза відкидається.

Статичний параметр, заданий рівнянням обчислюється для m = 4 і статистика повинна задовольняти умові:

$$1{,}03 < x_2 < 57{,}4$$

Тест серій

Під серією розуміється послідовність однакових символів, 1 чи 0. Суть тесту: на заданій довжині тестуємої поверхні здійснюється підрахунок серій довжиною 1, 2, 3, 4, 5, 6 елементів. Серії більш 6 розглядаються як 6.

Якщо послідовність випадкова, то кількість серій:

Довжина серій	Необхідний інтервал
1	2267-2733
2	1079-1121
3	502-748

4	223-402
5	90-223
6	90-223

Тест довжин серій

Суть у підрахунку перевірки максимальної довжини серій з однакових елементів. Якщо послідовність випадкова, то мах довжина серії не повинна перевищувати значення 34.

Лекція №17

Випадкові послідовності

1. Основні визначення випадкової послідовності.
2. Методи і засоби перевірки на випадковість.

Стійкість у визначеній мері залежить від джерела ключів. Теорія Симонсона і теорія Шенона базується на тім, що:

ключі породжуються джерелом випадково, (1)

порівняно ймовірно, незалежно й однорідно

Усі теоретичні твердження й оцінки справедливі в (1). Якщо умова не виконується, то стійкість може знижуватися до неприпустимих меж.

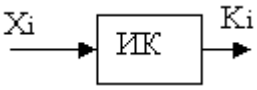


Рис.17.1

1. Визначення Шенона

Послідовність називається випадковою, якщо вона містить у собі максимальну інформацію (тобто в ній не міститься надмірність).

$$H(k) = -\sum_{i=1}^{n_K} P(k_i) \log P(k_i) \tag{2}$$

Можна показати, що extremum (2) досягається за умови, що:

$P_i = P_j \forall i, j$ - порівняно ймовірні

$$-\sum_{i=1}^{n_K} \frac{1}{n_k} \log_2 \frac{1}{n_k} = -n_k \frac{1}{n_k} \log_2 n_k^{-1} = \log_2 n_k \tag{3}$$

Якщо ключі породжуються порівняно ймовірно, то для КРА складність максимальна.

$$l_0 = \frac{H(k)}{r \log_2 m} \tag{4}$$

$$l_0 = \frac{H(k)}{r} \tag{4}$$

lo – відстань однозначності

$$ml_0 \to H \to H_{\max}$$

Для досягнення стійкості ключі повинні породжуватися порівняно ймовірно і випадково. Забезпечення умови, що в послідовності міститься максимум інформації еквівалентно тому, що ця послідовність не містить надмірності.

2. Визначення Холмогорова

Грунтується на складності обчислень. Послідовність називається випадковою по Холмогорову, якщо її складність дорівнює n, тобто її не можна сформувати з використанням алгоритму, довжина входу якого менше n.

Для того, щоб джерело ключа формував випадкову послідовність ми повинні подати на вхід n - символ ініціалізації, при цьому умові послідовність може бути як випадкової, так і псевдовипадкової.

. Визначення Блюма

Послідовність Y_i є випадкової, якщо не існує ніякого поліноміального алгоритму, за допомогою якого її можна відрізнити від еталонної випадковості. Таке визначення дозволяє працювати й оцінювати властивості конкретних послідовностей.

$$Y_i \to Y^7$$

Y_i - ПСП наближається до еталона.

Приклад:

$$LC_{i+1} = C_i^{E_K} (\mathrm{mod}\, N_j) \qquad (6)$$

$X_i \to N_j : E_K \qquad \mathrm{x_i} = x_0 \quad \mathrm{lx_0} = 512$

$LC_1 = X_0^{E_K} (\mathrm{mod}\, N_j)$

$LC_2 = C_1^{E_K} (\mathrm{mod}\, N_j)$

$Y_i = LC_1, LC_2, ...$

4 підхід

Базується на безлічі тестів. Послідовність називається випадковою (псевдовипадковою), якщо вона проходить деяку безліч незалежних тестів. Це єдиний підхід, що дозволяє зробити практичні оцінки.

Метод тестування на основі χ^2

Критерій χ^2 дозволяє перевірити погодженість гіпотетичних ймовірностей.

$$P_k = P(x_k)$$

$\mathrm{x_1}, \mathrm{x_2}, ... \mathrm{x_k}$ з їх відносними частотами $\mathrm{h}_\nu = \frac{V_K}{n}$ які визначаються над вибіркою з n - незалежних чи спостережень подій.

При використанні критерію спочатку визначається статистика χ^2.

$$\chi^2 = n \sum_{k=1}^{m} \frac{(h_K - P_K)^2}{P_K} \qquad (7)$$

де m- кількість інтервалів розбивки

Ухвалення рішення здійснюється на основі обчислення деякого граничного значення для рівня значимості α.

$$\chi_{\alpha}^{2} = l\left(1 - \frac{2}{9l} + Z_{\alpha}\sqrt{\frac{2}{9l}}\right) \quad (8)$$

l - кількість ступенів волі

Z_{α} - граничне значення стандартного нормального розподілу

Гіпотеза відкидається, якщо:

$$\chi^{2} > \chi_{\alpha}^{2} \quad (9)$$

Генератор псевдовипадкової послідовності на базі многомодульного перетворення

Генерується $\{P_1, P_2, P_3 .m\}$

$$\begin{cases} \text{выбирается } \Theta_{\nu} & \mathrm{Y}_{\mathrm{i}}^{/} = Y_{i-1}\Theta_{\nu} (\mathrm{mod}\, P_1) \\ Y_i'' = Y_i^{/} (\mathrm{mod}\, P_2) \\ Y_i''' = Y_i'' (\mathrm{mod}\, P_3) \\ Y_i = Y_i''' (\mathrm{mod}\, m) \end{cases} \quad (10)$$

Якщо P_i і m взаємнопрості, породжує псевдовипадкову послідовність з гарантованим періодом P_i-1.

Приклад:

Нехай генератор працює з частотою 10^{18} символів/секунду $P_1 \Rightarrow 2^{512}$

Визначимо t протягом який сформується послідовність:

$$t_b = \frac{10^{153}}{10^{18} * 3 * 10^{7}} = 3 * 10^{127} років$$

На відміну від (10) цей генератор можна розглядати $GF(P^m)$ й в окремому випадку $GF(2^m)$.

Нехай є $EC(GF(P^m))$, p – просте.

$$\{a, b, u, G, n\} \quad (11)$$

$$y^2 + xy \equiv x^3 + ax^2 + b(mf(x), p) \quad (12)$$

$$G_{i+1}^{/} = G_i^{/} * r_i (\mathrm{mod}\, f(x), p)$$

$$G_{i+1} = LG_{i+1}^{/}$$

$$G_{Li+1} = (X_{i+1}, Y_{i+1})$$

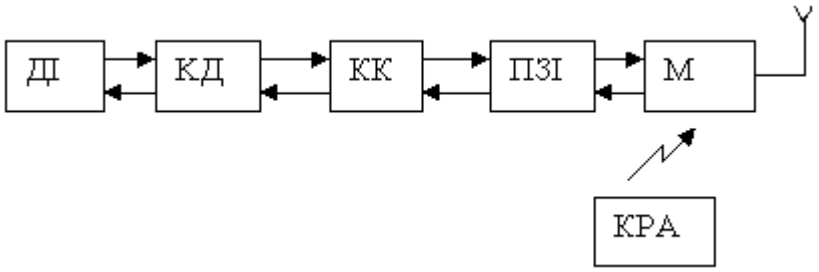
$$G_{i+1} = X_{i+1}$$

Лекція № 18

Проблемні питання автентифікації в каналах зв'язку

1. Поняття складного сигналу.
2. Теоретичні положення.
3. Оцінка автентичності.

У ряді систем необхідно забезпечити не тільки конфіденційність, цілісність і дійсність переданих команд, але і сам факт передачі цієї інформації в захищеному виді сховати. Цим займається стеганографія.



1 – джерело інформації

рис.18.1

2 – кодер джерела

3 – кодер канали

4 – пристрій захисту інформації

5 – модулятор (антена)

Кодер джерела забезпечує узгодження ДІ з пропускною здатністю каналу зв'язку, тобто інформація джерела представляється в цифровому виді, бажано виключити надмірність.

У $M_i^{/}$ виключена надмірність.

$$U(t) = \mu(t) * S(t) + R(t)$$

мультиплікативна складова перешкоди

адитивна складова перешкоди

Дія перешкод приводить до перекручувань у каналі зв'язку – імовірність $P_{пом/бит} = 10^{-k}$.

Кодер каналу призначений для внесення навмисної надмірності (стійкого до перешкод кодування) з тією метою, щоб використовуючи цю надмірність на прийомній стороні можна було б чи знайти (і) виправити цю надмірність.

ПЗІ призначено для забезпечення конфіденційності, цілісності і дійсності інформації. Реалізується цифровим підписом і т.д.

У модуляторі здійснюється заміна M_i - символів криптограми на сигнали переносники інформації, що добре поширюються в середовищі.

Припустимо, що захист інформації здійснюється в ПЗІ.

C_i 1 / 0

$$C_j(1) = S_1(t, \varphi_i)$$
$$C_j(0) = S_0(t, \varphi_i)$$

У таких системах треба забезпечити:

1) енергетична скритність (енергетики не вистачає, щоб знайти факт передачі сигналу).

$$\left(\frac{P_c}{P_n}\right)p_n$$

2) структурна скритність – стійкість сигналів, переданих у радіоканалі, протистояти виділенню з них параметрів і інформації.

3) стійкість до перешкод – як здатність системи протистояти впливу як випадкових, так і навмисних перешкод.

4) автентичність, дійсність, цілісність, тобто здатність протистояти передачі помилкової інформації, команд, чи модифікацій щирих команд у помилкові. Усім цим вимогам можуть задовольнити комплекс шумоподібних сигналів.

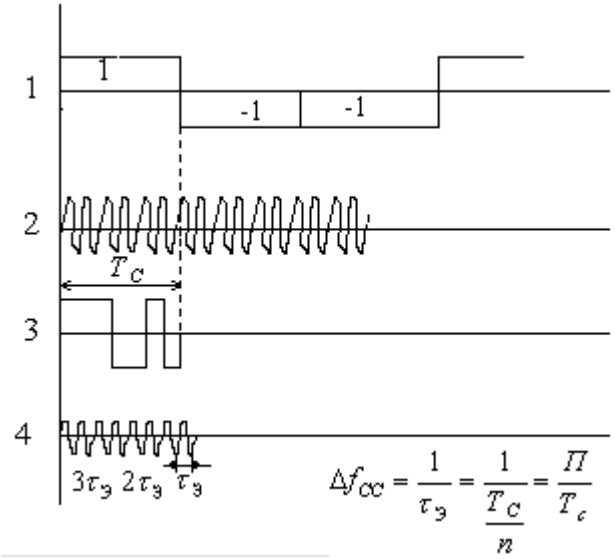


рис.18.2 – Епюри використання простих і елементарних складних сигналів.

ΔF - полоса пропущення сигналу

$$\Delta F_c = \frac{1}{T_c} \quad (1)$$

$$\Delta f_{CC} = \frac{1}{\tau_э} = \frac{1}{\frac{T_C}{n}} = \frac{П}{T_c} \quad (2)$$

$P_c > P_n$ - такі сигнали не є захищеними і немає енергетичної скритності.

Полоса частот складного сигналу збільшилася в n раз, але енергія сигналу збереглася. Щільність сигналу може стати набагато менше щільності перешкоди.

3 30

$$P_c << P_n$$

$$S(t) = S_0(\cos\omega_i t + \varphi_i)$$

Фаза і частота такого сигналу можуть мінятися за законом Тінф.

Теорема 1.

Нехай у радіосистемі здійснюється M_i - те кодування, при якому М біт інформації ставиться у відповідність 2^m сигналам складним, обираних з деякої безлічі {S}. Тоді, необхідною і достатньою умовою теоретичної недешифруємості системи є наступна умова:

$$\begin{cases} P\left(S_i / M_i\right) = P(S_i) \\ P\left(S_i / S_{i-1}, S_{i-2} \ldots.\right) = P(S_i) \end{cases} \qquad (3)$$

1. Імовірність появи S_i сигналу в каналі не повинна залежати від того, яке повідомлення з'явилося на виході джерела.
2. Імовірність появи сигналу в каналі не повинна залежати від того, які сигнали перед цим випромінювалися.

Радіоканали, у яких виконуються ці умови, називаються динамічними.

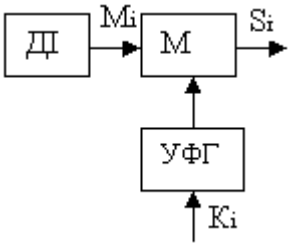


рис.18.3 - Структурна схема динамічного каналу

У такій системі імовірність обману можна оцінити:

$$P_{обм} = \frac{n_M}{n_C}$$

При $l_c = 10^3 \div 10^4$ можна забезпечити $n_M = 2^{l_M}$, $n_S = 2^{l_M + l_S}$ простір сигналів.

Лекція 19

Порядок оцінки вартості та автентичності динамічних радіоканалів.

1. Математична модель, структурна схема динамічного радіоканалу
2. Особливості формування складних сигналів
3. Формування Γ_y управляючих і ключових даних

1) Математична модель, структурна схема динамічного радіоканалу

В ряді систем управління необхідно реалізувати старт - стопний принцип управління, коли команди на виконання визначених функцій передаються послідовно з очікуванням підтвердження виконання цієї команди. Застосовувати традиційну апаратуру достатньо складно. Імітостійкість (цілістність і справжність) таких радіоліній буде недостатньою.

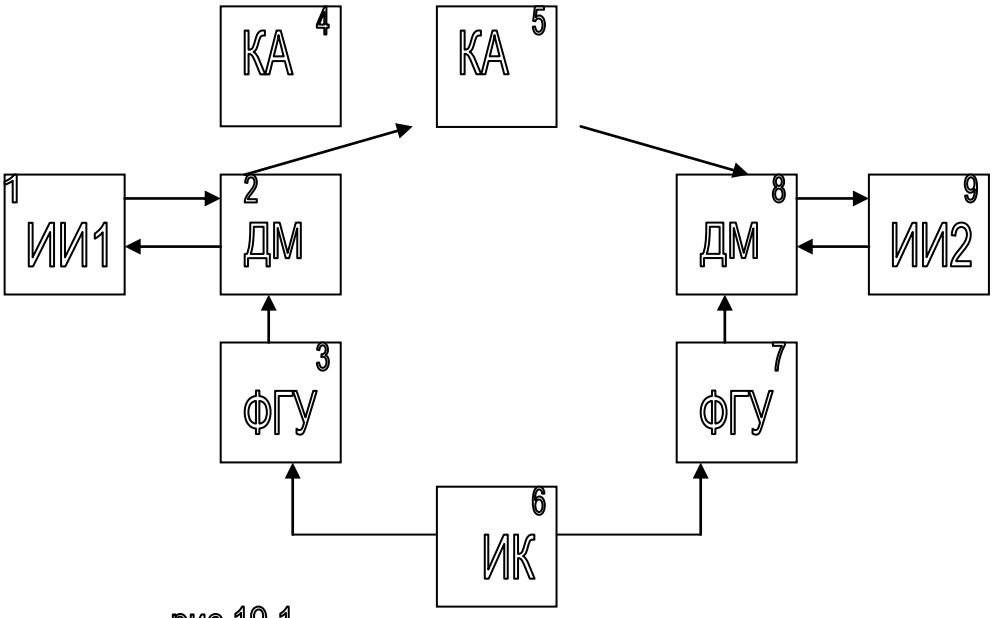


рис.19.1.

На рис. 21.1 приведена спрощена схема, принцип функціонування динамічного канала.

ДІ1, ДІ2 – джерело інформації

ДМ - динамічний модулятор

ФГУ - формувач Γ_y

ДК - джерело ключей

КА – космічний апарат

ДІ1 і ДІ2 є джерелами та отримувачами команд управління. Команди передаються старт – стопним режимом. Для криптозахисту з одночасним забезпеченням і конфіденціальності, і справжності, і цілістності застосовується динамічний режим передачі сигналів.

ДМ містить множину(ансамбль) складних сигналів {S} з розмірністю n_S .Формувач Γ_y в кожний момент Δt формує символ $\Gamma_ш$ ($\Gamma - шифруюча$) з основою алфавіту m. В наслідок із множини n_S сигналів по m-ічной Γ обирається m сигналів, які в заданому інтервалі є дозволеними для випромінювання і прийома на обох сторонах. Встановлення відповідності : m_i блок ДІ1 $\rightarrow m_{сиг}$ змінюється у відповідності з Γ

$$m_i = 2\begin{cases}1 \rightarrow S_i \\ 0 \rightarrow S_j\end{cases}$$

КА повинено бути засинхронізоване по Γ_y з тим, щоб розрізняти який із сигналів передається $S_i \ или \ S_j$ в коливанні.

$$S_i(t) - u(t) = \mu(t) \cdot S_v(t) + R(t) \qquad (19.1)$$

Схема розрізнення сигналів визначає який з сигналів $S_i \ або \ S_j$ передається в коливанні (рис.19.2).

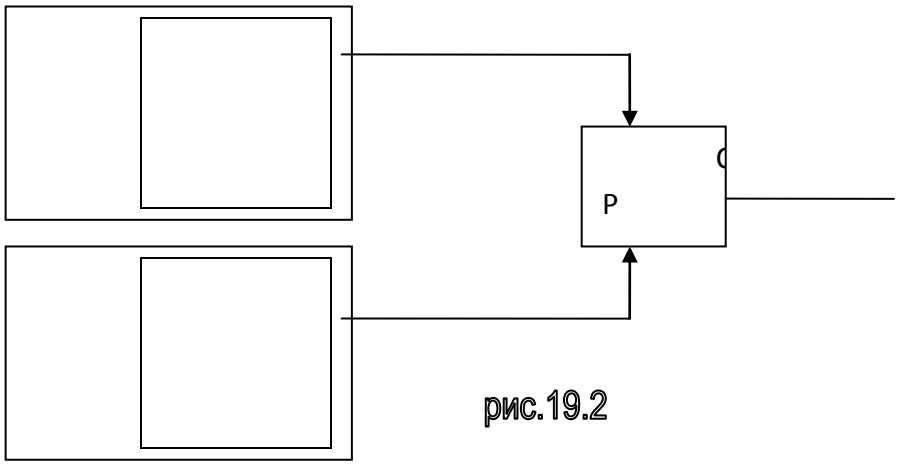


рис.19.2

$$Y_1 = \int_0^{T_c} u(t) \cdot S_i(t) dt$$

$$Y_2 = \int_0^{T_c} u(t) \cdot S_j(t) dt$$

СР (порівнювач) порівнює $Y_i \quad u \quad Y_j$. $Якщо Y_i > Y_j, то S_i \Rightarrow 1.$

$Якщо Y_i \le Y_j, то S_j \Rightarrow 0.$

Очевидно, формувач Γ_y повинен у заданий момент обрати правильно на борту і и j, такі ж як на Землі.

Особливості: для правильного обміну командами наземний ФГУ і ФГУ космічного апарату повинні обрати Γ_y узгоджено. Це здійснюється за рахунок:

1) використання довгострокових ключів;
2) використання сеансових ключів;
3) передачі синхромаркерів або управляючих послідовностей у кожній команді.

2) Особливості формування складних сигналів.

Частотна модуляція.

ДМ повинен формувати множину $S_\nu(t)$ сигналів.

$$S_\nu(t) = S_0 \cdot \cos(\omega_\nu \cdot t + \varphi)$$

Фазова модуляція.

$$S_\nu(t) = S_0 \cdot \cos(\omega_0 \cdot t + \varphi_i)$$

Частотно - фазова модуляція.

$$S_\nu(t) = S_0 \cdot \cos(\omega_\nu \cdot t + \varphi_i)$$

Линійна частотна модуляція.

$$S_\nu(t) = S_0 \cdot \exp G(\omega_i \cdot t + \frac{\mu \cdot t^2}{2} + \varphi_i)$$

$$S_\nu = S_0 \cdot \cos(\omega_i + \frac{\mu \cdot t^2}{2} + \varphi_i)$$

$$\mu = \frac{2 \cdot \pi \cdot f}{T_c}$$

Якість СР є $\frac{E_c \quad (енергія накоплення сигнала)}{N_0 (спектральна щільність потужності поміхи)}$.

$$\frac{E_c}{N_0} = \frac{P_c \cdot T_c}{P_П / \Delta F} = \frac{P_c \cdot T_c \cdot \Delta F}{P_П}$$

$T_c \cdot \Delta F = B_c$, де T_c - тривалість сигналу, ΔF - полоса частот, B_c - база сигналу.

Знайдемо B_c для простого сигналу:

$$\Delta F = \frac{1}{T_c}, \quad T_c \cdot \frac{1}{T_c}, \quad B_c = 1$$

Із виразу $\frac{P_c \cdot T_c \cdot \Delta F}{P_П}$ випливає, що для того щоб можна було б розрізняти сигнали з $P_c < P_П$ необхідно, щоб $B_c > 1$

$$\Delta F = \frac{1}{\tau_э} = \frac{1}{T_c / l} = \frac{l}{T_c}, \quad де\, l - кількість\, елементів\, \tau_э\, в\, складному\, \; сигналі$$

$$B = T_c \cdot \Delta F_c = T_c \cdot \frac{l}{T_c} = l$$

B =кількості символів складного сигналу. Збільшуючи $B = T_c \cdot \Delta F_c = l$ відповідним чином, можна забезпечити потрібне $\frac{E_c}{N_0}$, при $\frac{P_c}{P_П} < 1$, тобто сигнал буде під шумом.

Характеристики для ДМ:

1. Вид модуляції складного сигналу(спосіб формування)

2. Кількість складних сигналів n_S, які можуть бути створені в модуляторі.

3. Складність створення складного сигналу в реальному масштабі часу.

Формування складного сигналу здійснюється на основі використання дискретних сигналів маніпуляції. Якщо здійснюється ФМ, то дискретний сигнал маніпуляції визначає закон створення складного ФМ сигналу.

Висновок: застосування складних сигналів дозволяє :

1.розрізняти сигнали, тобто приймати інформацію при $\frac{P_c}{P_П} < 1$;

2.так як $\frac{P_c}{P_П} < 1$, то такий сигнал володіє енергетичною скритністю;

3.оскітьки існує множина різних форм складних сигналів, то це можна використати для зменшення $P_{\frac{нав}{сиг}}$, тобто для зменшення імітозахисту.

В якості маніпуліруючих сигналів W_i повинні використовуватись сигнали з добрими авто- і взаємно кореляційними функціями.

Класи W_i :

1. Лінійні і нелінійні рекурентні послідовності.
2. Ортогональні і довільні ортогональні послідовності.
3. Квазіортогональні послідовності з самосинхронізацією.

3) Формування Γ_y управляючих і ключових даних

Γ_y повинна володіти таким ж стандартними властивостями, як і $\Gamma_ш$:

1. $l_\Gamma \geq l_o$;

2. Основа алфавіту повинна бути m – ічної;

3. Структурна скритність $S_\Gamma \geq S_o$, $где\, S_\Gamma = \frac{l}{L}$, l – кількість символів Γ_y, які необхідно правильно перехватити, для того щоб розкрити закон формування , що залишились L-l, ідеальний випадок - $S_\Gamma = 1,\ L = l$;

4. Повинна існувати можливість синхронізації Γ_y у просторі і часі.

Основною характеристикою такого каналу є $P_{\frac{нав}{сиг}}$ - це ймовірність може бути оцінена як

$$P_{\frac{нав}{сиг}} = \frac{m}{n_S}.$$

Якщо в системі використовується авто- і ізоморфізми лінійної рекурентної послідовності максимального періоду, то $n_S = (\frac{\varphi(2^m - 1)}{2^m}) \cdot l_S$, де m – порядок розширення поля, а l_S - довжина послідовності.

Література

1. Карпінський М.П., Кінах Я. І. Оцінка рівня надійності системи шифрування RSA методом факторизації // Автоматика. Автоматизация. Электротехнические комплексы и системы. - 2000. - №2. - С. 91-94.
2. Карпінський М.П., Кінах Я. І. Використання методів факторизації для оцінки надійності системи шифрування RSA // Радиотехника .- 2000. - №114. - С. 107-110.
3. Карпінський М.П., Кінах Я. І. Використання паралельних обчислень для криптоаналізу асиметричних систем шифрування Ель-Гамала та RSA // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - 2001. - №2.- С. 155-158.
4. Карпінський М.П., Кінах Я. І. Криптографія без обміну ключами // Тези доповідей четвертої наук.-техн. конф. “Прогресивні матеріали, технології та обладнання в машино- і приладобудуванні”. - Тернопіль: ТДТУ. - 2000. - С. 132.
5. M. Karpinsky., Y. Kinakh Reliability of RSA algorithm and its computational complexity // Computing. – 2003. - Vol 2. - Issue 3. – P. 119-122.