СИМЕТРИЧНІ КРИПТОСИСТЕМИ

студентка групи СНс-43
Суханя Галина

Симетричні криптосистеми – спосіб шифрування, в якому для шифрування і дешифрування застосовується один і той же криптографічний ключ. Ключ алгоритму повинен зберігатися в секреті обома сторонами.

Класифікація симетричних криптоалгоритмів

Симетричні криптоалгоритми:

1 ПОТОКОВІ ШИФРИ

Головною рисою потокових шифрів є побітна обробка інформації. Шифрування і дешифрування в таких схемах може обриватися в довільний момент часу, як тільки з'ясовується, що потік що передається перервався, і також відновлюється при виявленні факту продовження передачі.

Найбільш поширеними представниками потокових шифрів являються скремблери.

1.1 СКРЕМБЛЕР

Скремблер (від англ. Scramble - перемішувати, збивати) - це набір біт, які міняються на кожному кроці по визначеному алгоритму.

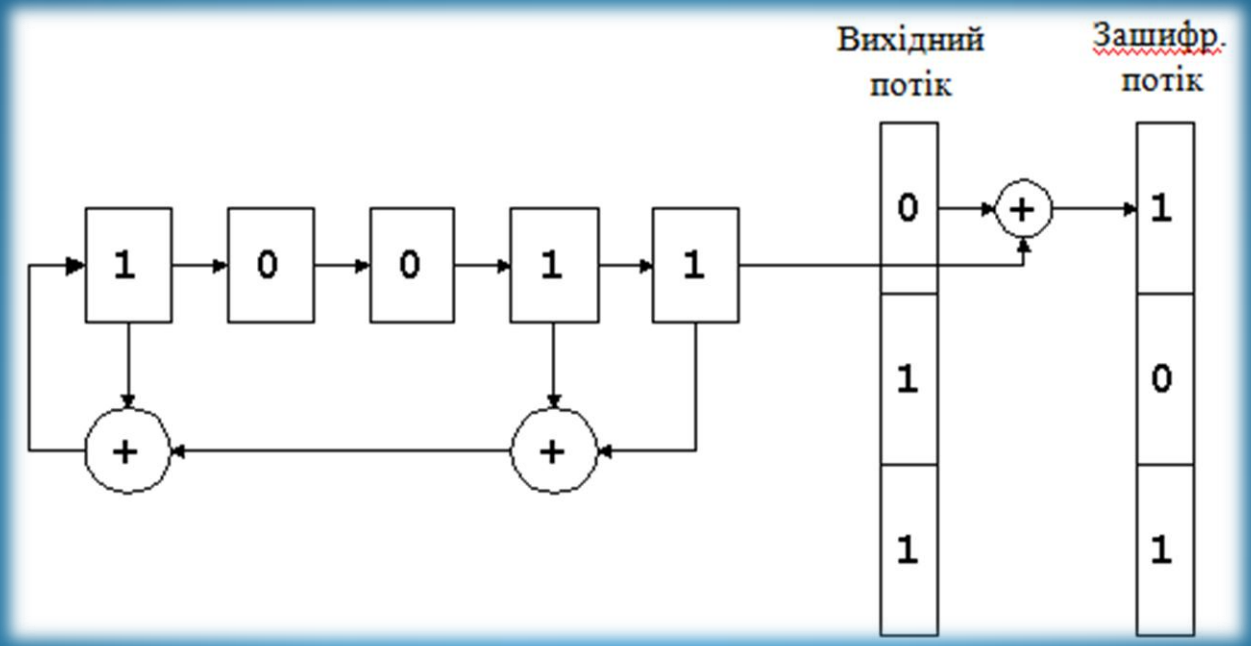

Схема шифрування інформації

Симетричні криптоалгоритми:

2 БЛОЧНІ ШИФРИ

Характерною особливістю блочних криптоалгоритмів є той факт, що в ході своєї роботи вони виробляють перетворення блоку вхідної інформації фіксованої довжини і отримують результуючий блок того ж обсягу.

Блокові шифри є основою, на якій реалізовані практично всі криптосистеми. Методика створення ланцюжків із зашифрованих блочними алгоритмами байт дозволяє шифрувати ними пакети інформації необмеженої довжини.

2.1 Шифр TEA

Шифр TEA (Tiny Encryption Algorithm) – один із самих простих в реалізації, але стійких криптоалгоритмів.

Відмінною характеристикою TEA є його розмір, простота операцій, відсутність табличних підстановок і оптимізація під 32-розрядну архітектуру процесорів.

Недоліком алгоритму є деяка повільність, пов'язана з необхідністю повторювати цикл Фейштеля 32 рази (це необхідно для ретельного «перемішування даних» через відсутність табличних підстановок).

2.2 Мережа Фейштеля

Мережа Фейштеля – метод оборотних перетворень тексту, при якому значення, обчислені від однієї з частин тексту, накладається на інші частини. Часто структура мережі виконується таким чином, що для шифрування і дешифрування використовується один і той же алгоритм - різниця полягає лише в порядку використання матеріалу ключа.

2.3 Стандарт AES

Стандарт AES – стандарт блочних шифрів США з 2000 року.

5 кращих представників, що пройшли в "фінал" змагання конкурсу AES:

Алгоритм	Творці	Країна	Швидкодія (asm, 200МГц)
MARS	IBM	US	8 Мбайт/с
RC6	R.Rivest & Co	US	12 Мбайт/с
Rijndael	V.Rijmen & J.Daemen	BE	7 Мбайт/с
Serpent	Universities	IS, UK, NO	2 Мбайт/с
TwoFish	B.Schneier & Co	US	11 Мбайт/с

Порівняння з асиметричними криптосистемами

Переваги:

- ✓Простота реалізації (за рахунок більш простих операцій);
- ✓Швидкість (на 3 порядки вища);
- ✓Менша довжина ключа для порівнянної стійкості ;
- ✓Вивченість (оскільки старші).

Порівняння з асиметричними криптосистемами

Недоліки:

- Складність управління ключами у великій мережі;
- Складність обміну ключами.

Перелік використаних джерел:

1. http://uk.wikipedia.org/wiki/Криптографія.
2. http://www.citforum.ru/internet/infsecure/ Методы и средства защиты информации.
3. http://itbezopasnost.ru/kriptografiya.html.