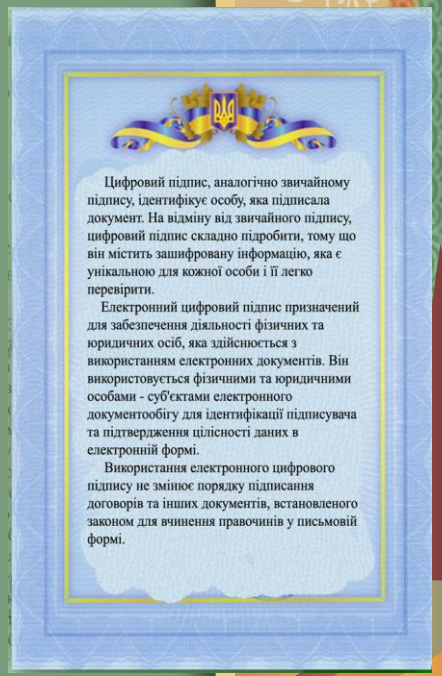
Доповідь на тему: “Технологія цифрових підписів”

Виконала:
студентка групи СНс-43
Пенюта Оля

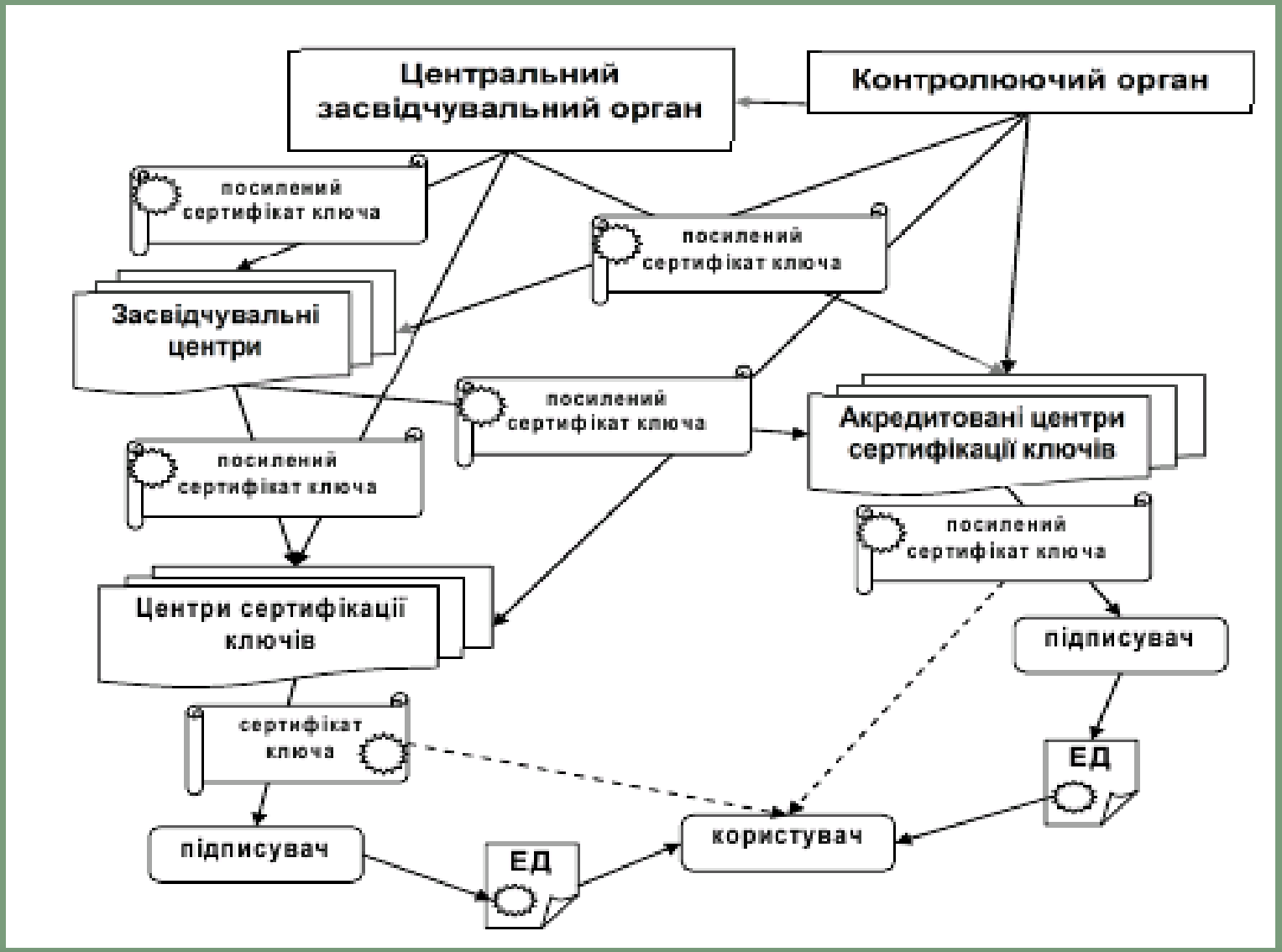
- Відповідно до статті 5 Закону України «Про електронні документи та електронний документообіг» *електронний документ* – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа.
- Обов’язковим реквізитом електронного документа є обов’язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили.
- Електронний підпис є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу. Накладанням електронного підпису завершується створення електронного документа. Відносини, пов'язані з використанням електронних цифрових підписів, регулюються законом. Використання інших видів електронних підписів в електронному документообігу здійснюється суб'єктами електронного документообігу на договірних засадах.


Цифровий підпис, аналогічно звичайному підпису, ідентифікує особу, яка підписала документ. На відміну від звичайного підпису, цифровий підпис складно підробити, тому що він містить зашифровану інформацію, яка є унікальною для кожної особи і її легко перевірити.

Електронний цифровий підпис призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів. Він використовується фізичними та юридичними особами - суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Використання електронного цифрового підпису не змінює порядку підписання договорів та інших документів, встановленого законом для вчинення правочинів у письмовій формі.

Електронний цифровий підпис (ЕЦП) — реквізит електронного документа, призначений для посвідчення джерела даних і захисту даного електронного документа від підробки.



Вигляд цифрових підписів

Lisa Jones

Автор цифрового підпису Lisa Jones
DN: cn=Lisa Jones, o=Kahili Coffee Company, ou=Відділ маркетингу, email=lisa@kahili.com, c=US
Причина: я переглянула цей документ.
Дата: 2006.08.07 09:59:53 -07'00'

Автор цифрового підпису Lisa Jones
DN: cn=Lisa Jones, o=Kahili Coffee Company, ou=Відділ продажів
Причина: я переглянула цей документ.
Дата: 2004.07.14 13:17:03 -07'00'

- **Алгоритми ЕЦП:**
- Американські стандарти електронного цифрового підпису: DSA, ECDSA.
- Російські стандарти електронного цифрового підпису: ГОСТ Р 34.10-94 (в даний час не діє), ГОСТ Р 34.10-2001.
- Український стандарт електронного цифрового підпису: ДСТУ 4145-2002.
- Стандарт PKCS#1 описує, зокрема, схему електронного цифрового підпису на основі алгоритму RSA.

Схема цифрового підписування за методом ECDSA

Той, хто підписує

Формування цифрового підпису

Обчислити геш-код h від повідомлення M
h = H(M)

Обчислити передпідпис R = kP

Обчислити добуток координати x_R, точки ЕК R на геш-код h, який попередньо перетворений на елемент поля. Результат перетворити на велике ціле число r

Обчислити велике ціле число z = dr mod n

Обчислити точку ЕК L = zP і перетворити координату x точки L на ціле число

Обчислити ціле число s за формулою
s = m'(r + h) mod n

Перетворити множину цілих чисел (s, r) на цифровий підпис DS = (0 || s || 0 || r)

M, DS

Той, хто перевіряє

m, E(A, B), P, n, Q, H

Перевірка цифрового підпису

Обчислити гед-код h від повідомлення M
h = H(M)

Перетворити цифровий підпис DS на множину цілих (s, r)

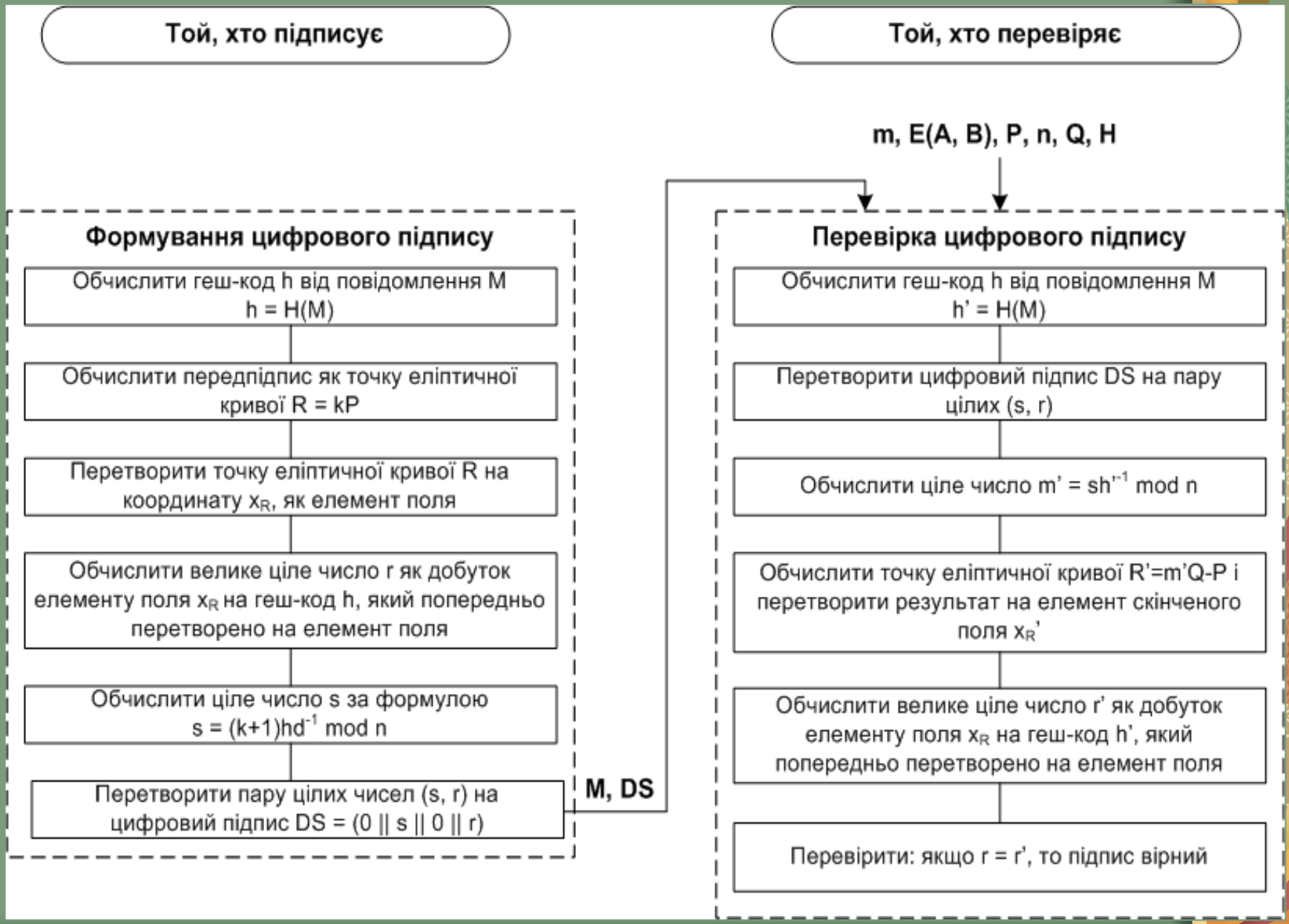
Обчислити точку ЕК L' = rQ і перетворити координату x точки L' на ціле число m''

Обчислити r' = (s - m''h') mod n

Обчислити r'' = rm'' mod n

Перевірити: якщо r' = r'', то підпис вірний.

Схема цифрового підписування за методом RSA



Сертифіковані засоби криптографічного захисту інформації:

1. Програмний виріб «Стандарт-Ява»
2. Програмний виріб «LS-crypt»
3. Бібліотека функцій криптографічних перетворень «УНІС-Альтінг»
4. Програмний виріб «Шифр»
5. Програмне забезпечення апаратно-програмних засобів електронного цифрового підпису «Основа»
6. Виріб програмний «Шифр+»
7. Апаратно-програмний засіб криптографічного захисту інформації «Старт»
8. Засіб програмний «Бібліотека криптографічних перетворень для операційних систем Windows, LINUX x86, MALLOW LINUX ARM «MxCrypt»
9. Програмний виріб «NovaLib»
10. Бібліотека програмних процедур криптографічного захисту інформації «Тайфун-W32»
11. Виріб програмний «Мебіус-Захист».
12. Засіб програмний «НДІ ПІТ КРИПТО».

ЗАКОН УКРАЇНИ

Про електронний цифровий підпис

(Відомості Верховної Ради України (ВВР), 2003, N 36, ст.276)
{ Із змінами, внесеними згідно із Законом
N 879-VI (879-17) від 15.01.2009, ВВР, 2009, N 24, ст.296 }

Цей Закон визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису.

...

Президент України Л.КУЧМА

м. Київ, 22 травня 2003 року
N 852-IV

Перелік літературних джерел

- http://help.adobe.com/uk_UA/Acrobat/9.0/Professional/WS58a04a822e3e50102bd615109794195ff-7d4a.w.html (24 березня 2010 року)
- http://www.unis.org.ua/index.php/uk/topcsk/questions (24 березня 2010 року)
- http://businesidea.ks.ua/rosiyany-oderzhaly-pravo-na-tsyfrovyj-pidpys/ (24 березня 2010 року)
- http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=39217&cat_id=39136 (9 квітня 2010 року)

Дякую за увагу!