

Введення у криптографію

Частина матеріалів "запозичені" від
DistributedLab

Криптографія

Криптографія – наука про методи забезпечення послуг інформаційної безпеки.

Криptoаналіз - наука про методи отримання секретних ключів, а також про методи виявлення вразливостей криптографічних алгоритмів та їх експлуатації.

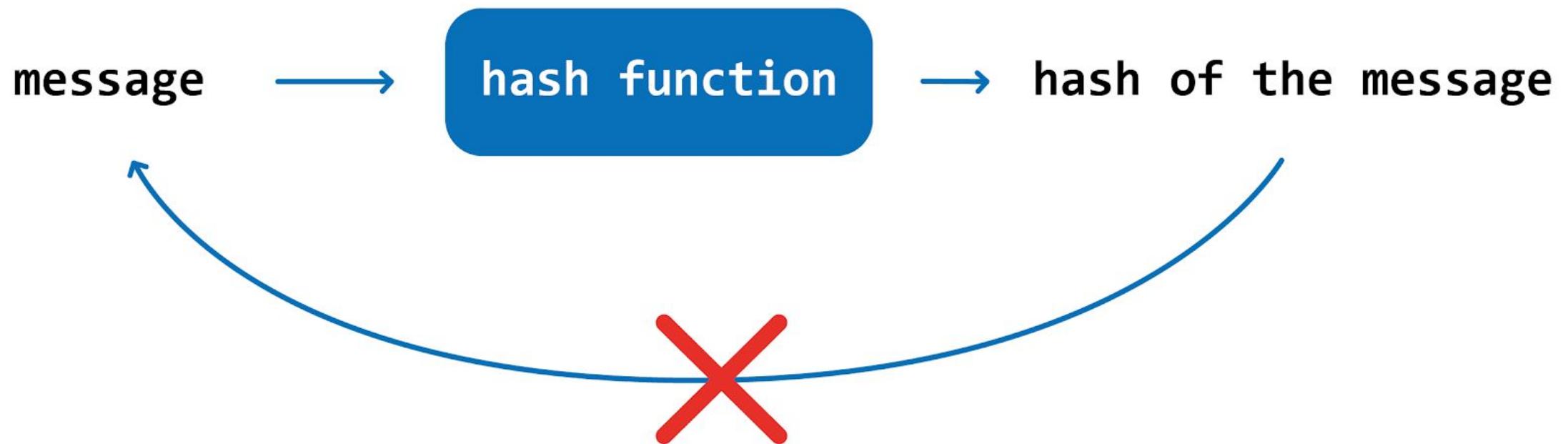
Постквантова криптографія - це розділ, який вивчає такі математичні схеми перетворення, на основі яких можна побудувати криптографічні схеми, стійкі до атак із використанням квантового комп'ютера.

Типи криптографічних перетворень:

- Хешування (гешування)
- симетричне шифрування
- асиметричне шифрування
- цифровий підпис

Хешування

Хеш-функція – це функція перетворення масиву вхідних даних довільної довжини у вихідний бітовий рядок фіксованої довжини, яка виконується за допомогою певного алгоритму.



Вимоги до хеш-функцій

- Стійкість до пошуку першого прообразу (неможливо відновити вихідне повідомлення за адекватний проміжок часу, знаючи лише хеш-значення, що відповідає йому)
- Стійкість до пошуку другого прообразу (сторона, що має вихідне повідомлення та відповідне йому хеш-значення, не може створити інше повідомлення, яке на виході хеш-функції надасть той самий результат)
- Стійкість до колізій
- (дод. Властивість/вимога) зміна одного біта на вході повинна призводити до зміни в середньому половині вихідних бітів

Хеш Функції. Колізії

30041001

10004301



silly
hash function

3+0+0+4+1+0+0+1



9



silly
hash function

1+0+0+0+4+3+0+1



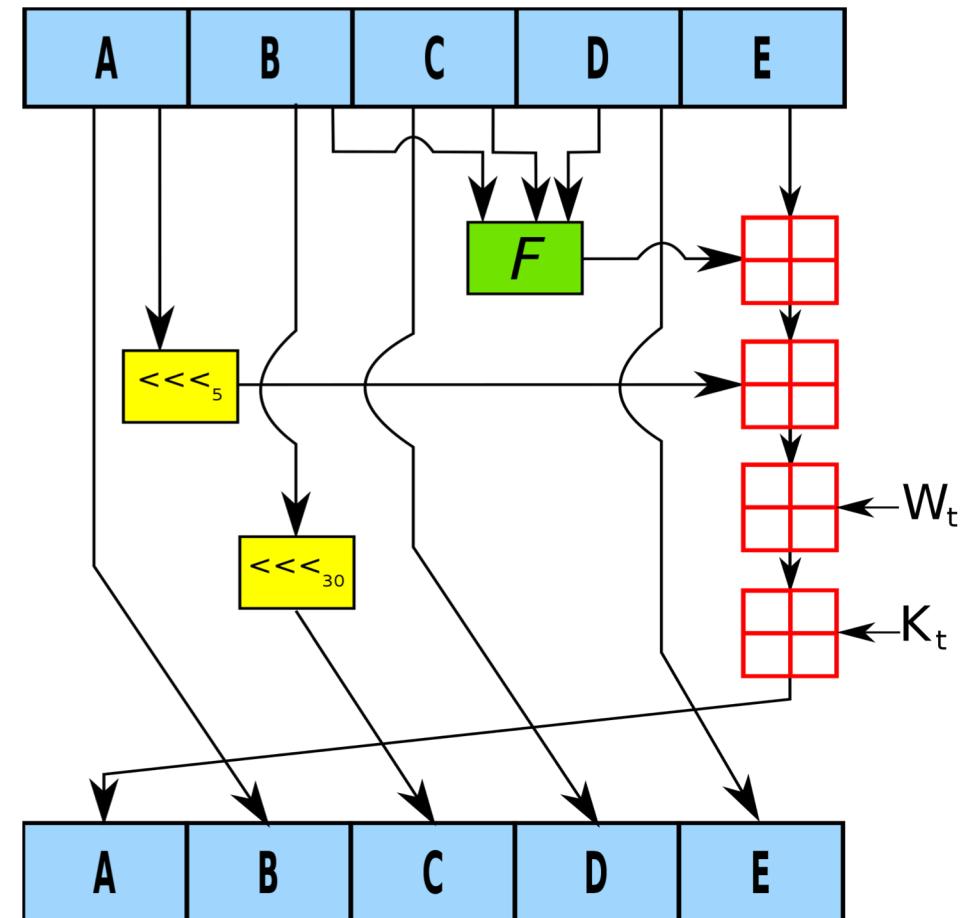
9

Область застосування хеш-функцій

- Контрольні суми передачі файлів
- Отримання унікального ідентифікатора набору даних
- Пошук дублікатів
- Цифровий підпис
- Зберігання паролів

Хеш-функції

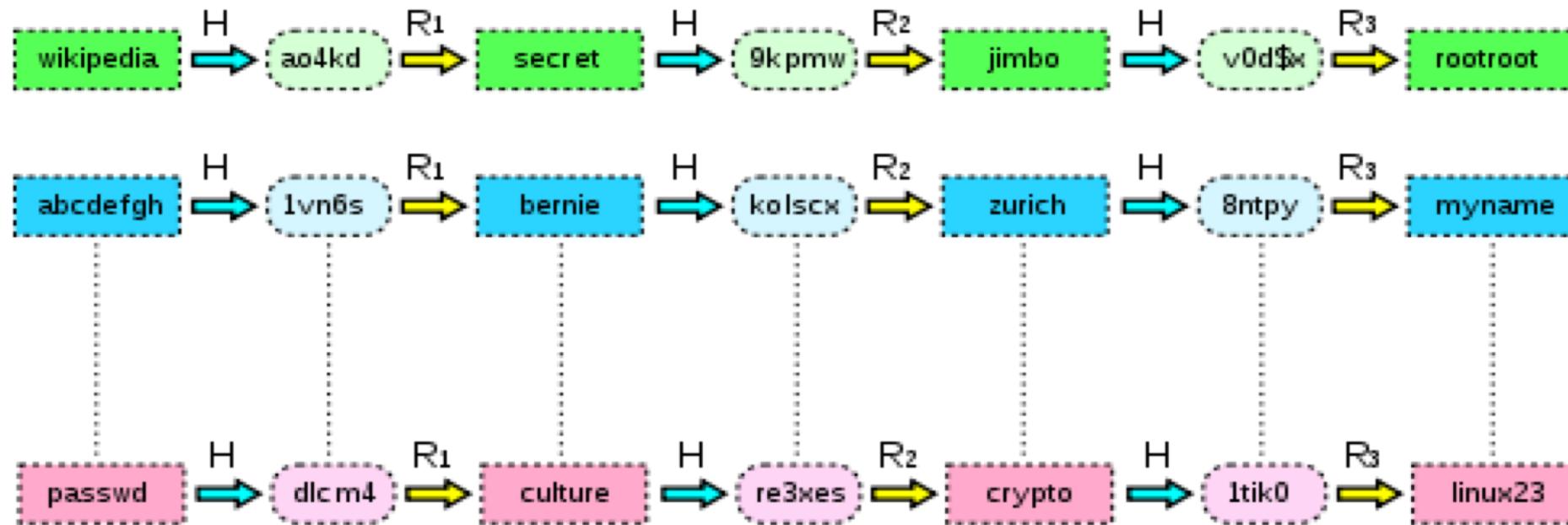
- Cyclic redundant check (CRC):
 - CRC16, CRC32
- Message-Digest Algorithm (MD):
 - MD2, MD5, MD6
- Message authentication code (MAC):
 - HMAC, OMAC, KMAC
- Secure hash algorithm (SHA):
 - SHA1, SHA-256
- BCrypt / SCrypt



MD5

- 128-бітний алгоритм хешування
- Типи зламу (злому):
 - Brute-force (Атаки перебірного типу)
 - Розмір БД = 2^{128} записів по (128 біт (хеш) + ~128 біт (текст)) => більш ніж 10^{29} ГБ
 - Алгоритмічна складність : при переборі $33 \cdot 10^6$ варіантів в секунду – повний перебір складатиме 10^{21} років
 - Межа Ландауера
 - Перебір за словарем
 - Rainbow crack
- Які результати будуть для 256-бітових алгоритмів?

Райдужні таблиці



Захист: використання «солей»
хеш = MD5(пароль + сіль)

Посилення захисту:
for 1 to X do
хеш = MD5(хеш + пароль + сіль)

Особливості: райдужні таблиці створюються тільки для одного «алфавіту», який характеризується набором можливих символів, що використовується у вхідній послідовності

Crypt (PHC, MCF) string format

```
$2b$[cost]$[22 character salt] [31 character hash]
```

man 5 crypt

For example:

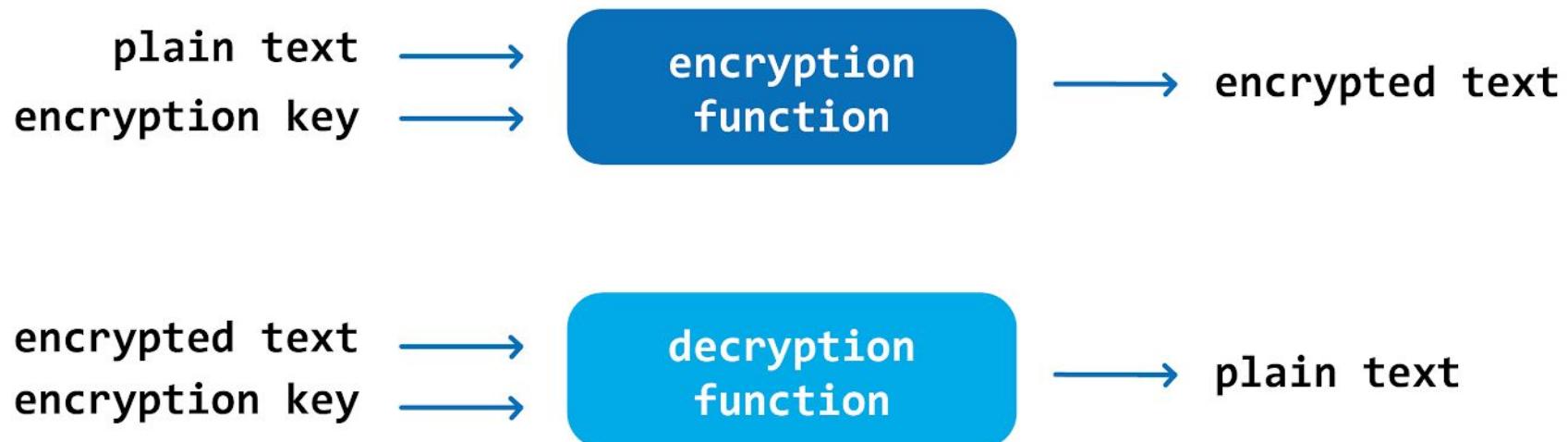
```
$2a$10$N9qo8uL0ickgx2ZMRZoMyeIjZAgcfl7p92ldGxad68LJZdL17lhWy  
\_/_\ \_/\_\_/\_\_/  
Alg Cost Salt Hash
```

Where:

- `$2a$` : The hash algorithm identifier (bcrypt)
- `10` : Cost factor ($2^{10} \Rightarrow 1,024$ rounds)
- `N9qo8uL0ickgx2ZMRZoMye` : 16-byte (128-bit) salt, base64 encoded to 22 characters
- `IjZAgcfl7p92ldGxad68LJZdL17lhWy` : 24-byte (192-bit) hash, base64 encoded to 31 characters

Симетриче шифрування

- **шифрування** – це видозміна тексту (або будь-яких інших даних) таким чином, що тільки той, хто має відповідний ключ, має можливість відновити вихідний текст.



Симетричне шифрування

Приклади:

- Шифр Цезаря
 - $Y = (X + k) \% N$, X – символ відкритого тексту, Y – символ шифрованого тексту, n – потужність алфавіту, k – ключ
 - Шифрування з використанням ключа k = 3.
 - Початковий алфавіт: А Б В Г Д Е Ї Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Й Ь Э Ю Я
 - Шифрований алфавіт: Г Д Е Ї Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Й Ь Э Ю Я А Б В
- Шифр Віженера
 - $C[i] = (m[i] + k[i]) \% n$, n – кількість літер в алфавіті, m – оригінальний текст, k – ключ
 - Початковий текст: ATTACKATDAWN
 - Ключ: LEMONLEMONLE
 - Шифрований текст: LXFOPVEFRNHR
- AES, DES
- Blowfish

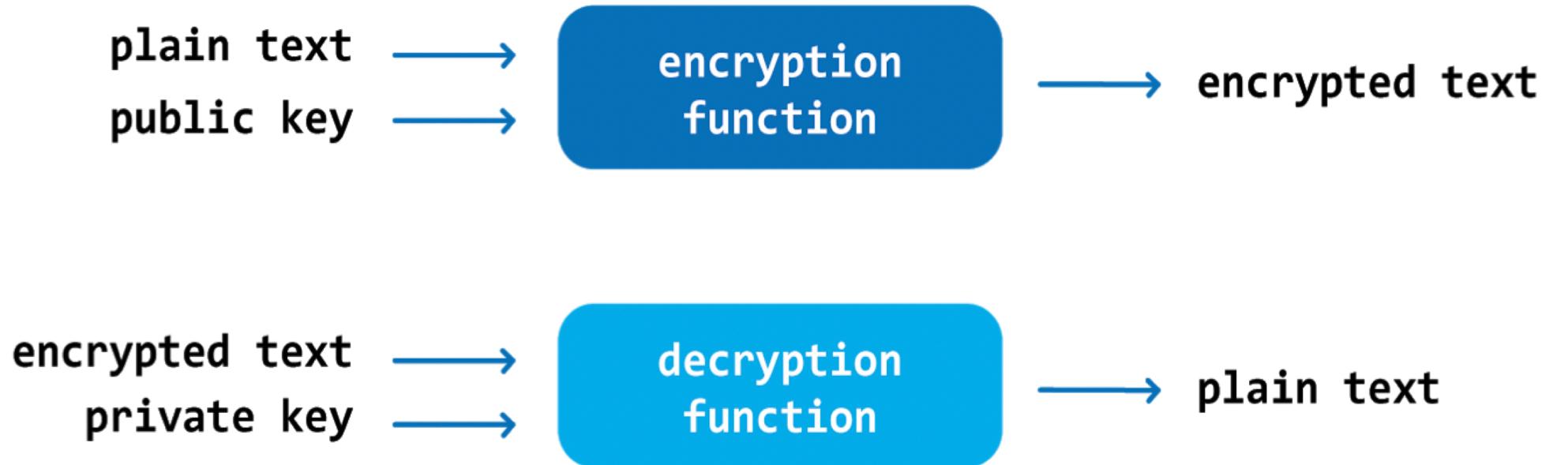
Проблеми:

- необхідність забезпечення конфіденційності секретного ключа під час його передачі одержувачу повідомлення ще до початку комунікації
- складність створення та зберігання нового ключа для кожного нового учасника в системі, де використовується захищена комунікація, заснована лише на симетричному шифруванні

ТИПИ СИМЕТРИЧНОГО ШИФРУВАННЯ

- Блокове шифрування
 - Техніка блокового шифрування включає шифрування одного блоку тексту за раз, тобто по одному. Так само розшифруйте текст, беручи один блок за іншим.
 - Звичайний розмір блоку може бути 64 або 128 бітів
 - використовує як плутанину, і дифузію
 - використовує режими алгоритмів ECB (електронна кодова книга) і CBC (ланцюжок блоків шифрів)
 - використовує той самий ключ для шифрування кожного блоку
- Потокове шифрування (Rivest Cipher (RC))
 - Технологія потокового шифрування включає шифрування і дешифрування одного байта тексту за раз.
 - Розмір блоку 1 байт (8 біт)
 - покладається лише з плутанину
 - використовує режими алгоритму CFB (Cipher Feedback) і OFB (Output Feedback)
 - використовує функцію XOR для перетворення звичайного тексту на зашифрований текст, тому легко звернути біти XORED
 - використовує різні ключі кожного байта

Асиметричне шифрування



```
openssl genrsa -des3 -out private.pem 2048  
openssl rsa -pubout -in private.pem -out public.key
```

Алгоритм RSA

- $\text{cipher} = \text{origin} ^ e \% n$
- $\text{origin} = \text{cipher} ^ d \% n$
- $(d \cdot e) \% \phi(n) = 1$
- $\phi(n) = (p - 1) \cdot (q - 1)$
- p, q – прості числа
- $e = \{17, 257, 65537\}$

Життєвий цикл ключа



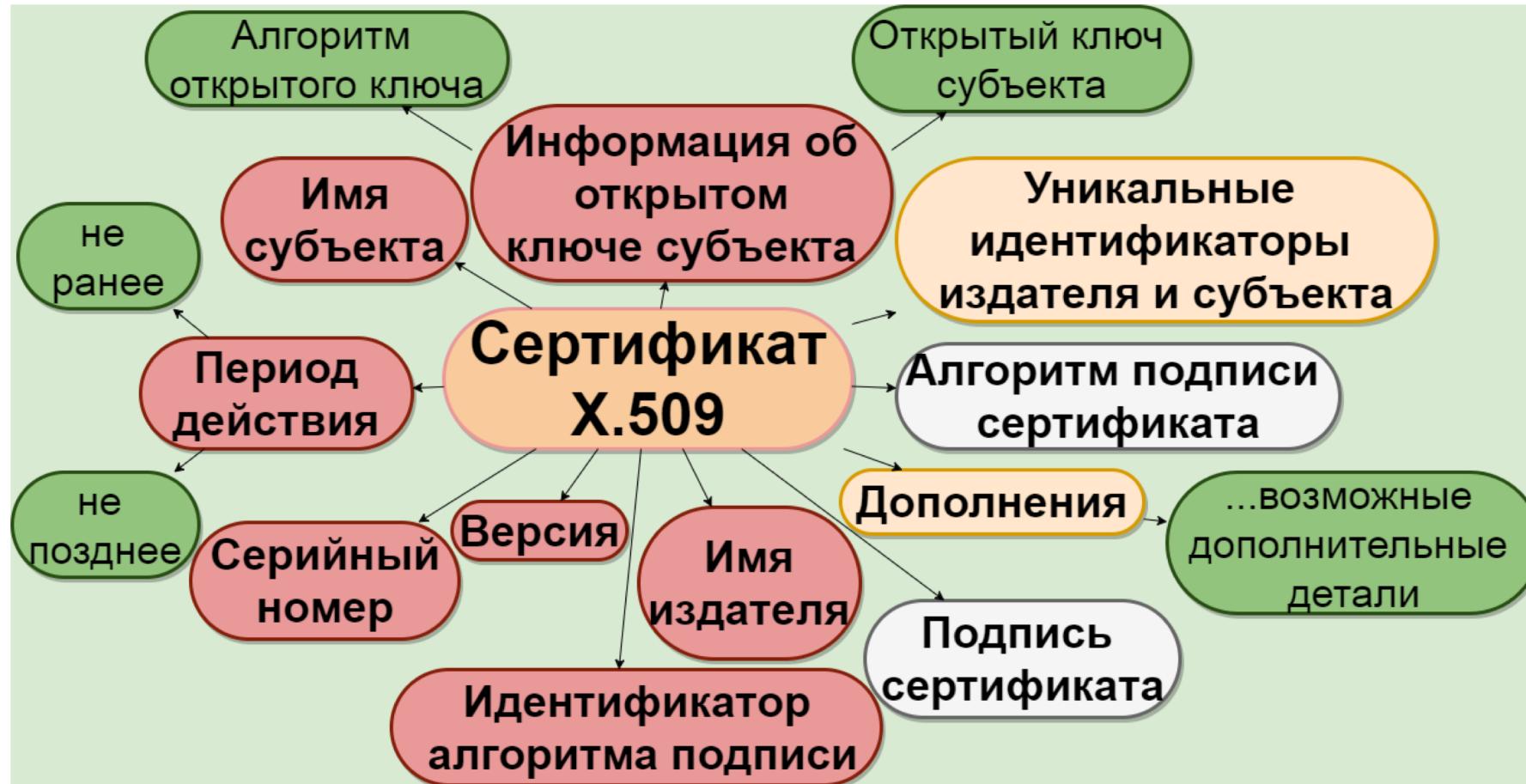
Генерація:

- З використанням генератора випадкових чисел (програмних, апаратних)
- Породження з іншого ключа (ієрархічна генерація ключей)
- Узгодження загального ключа
- Мнемонічні фрази (bip39)

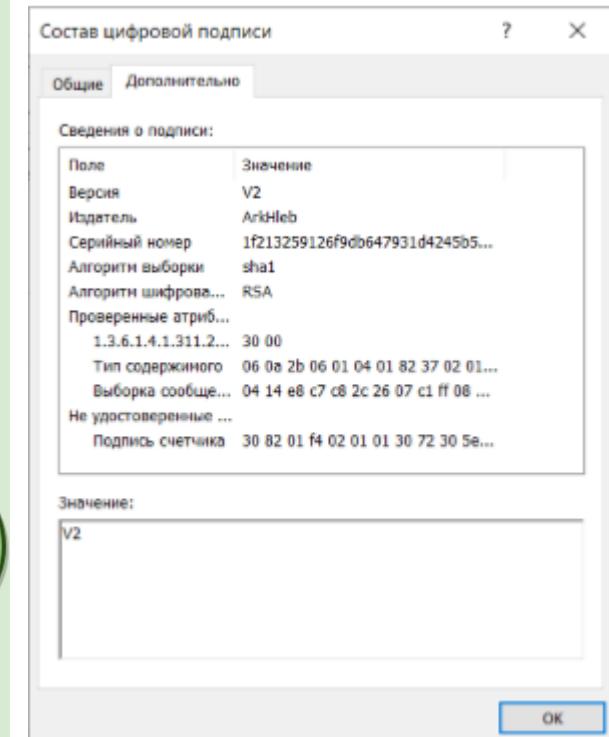
Інфраструктура відкритих ключів

- Безпечно способи обміну публічними ключами :
 - Особиста зустріч
 - Раніше використовуваний ключ
 - Третя довірча сторона

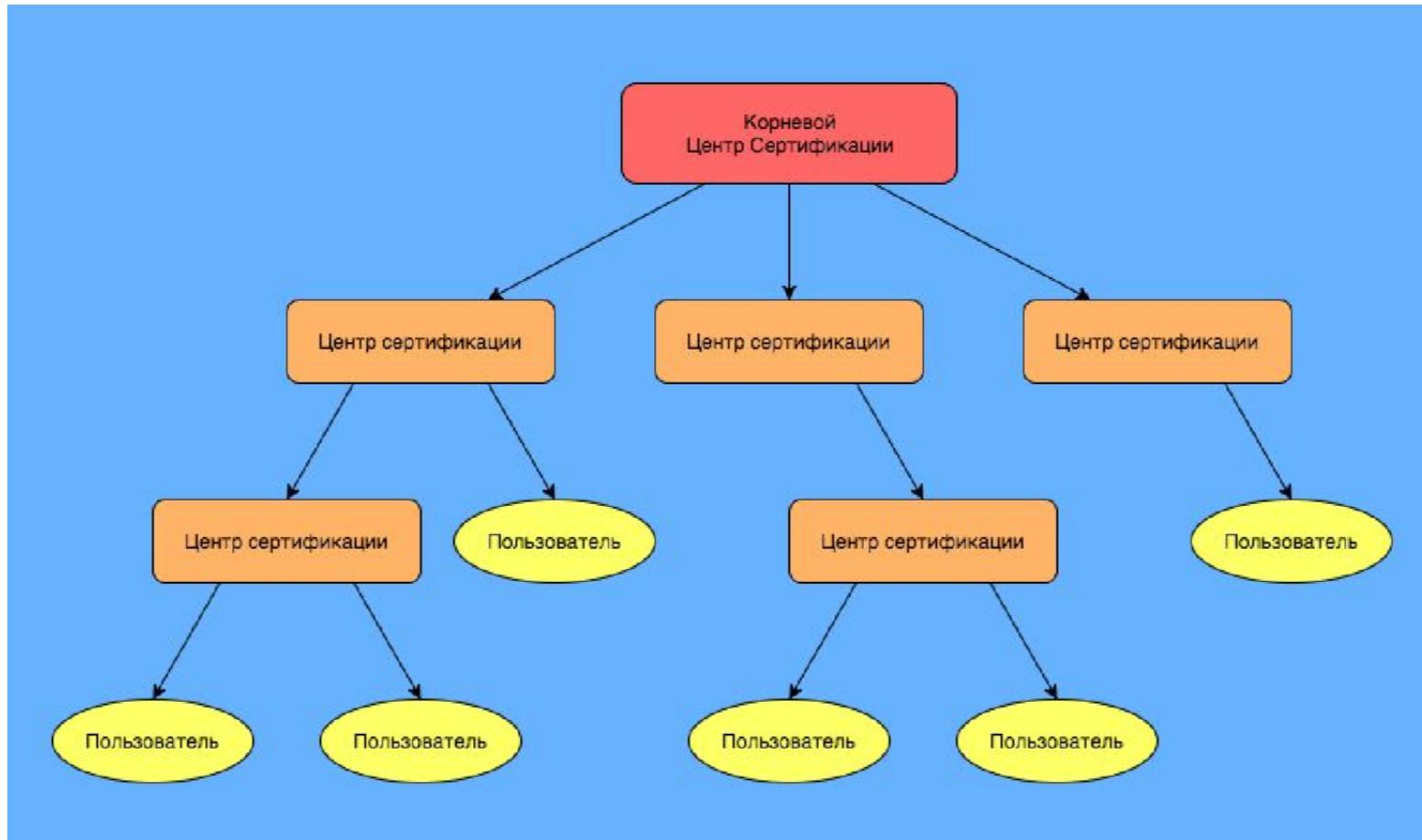
X.509 Сертифікат



```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365
```



Центри сертифікації



Обов'язки:

- Публікація критеріїв видачі сертифікатів.
- Надання сертифікатів заявникам, які відповідають опублікованим критеріям
- Управління сертифікатами (наприклад, реєстрація, оновлення та аннулювання)
- Збереження кореневих ключів.
- Перевірка доказів, поданих заявниками.
- Надання коштів для реєстрації.
- Прийняття відповідальності, пов'язаної з цими обов'язками.

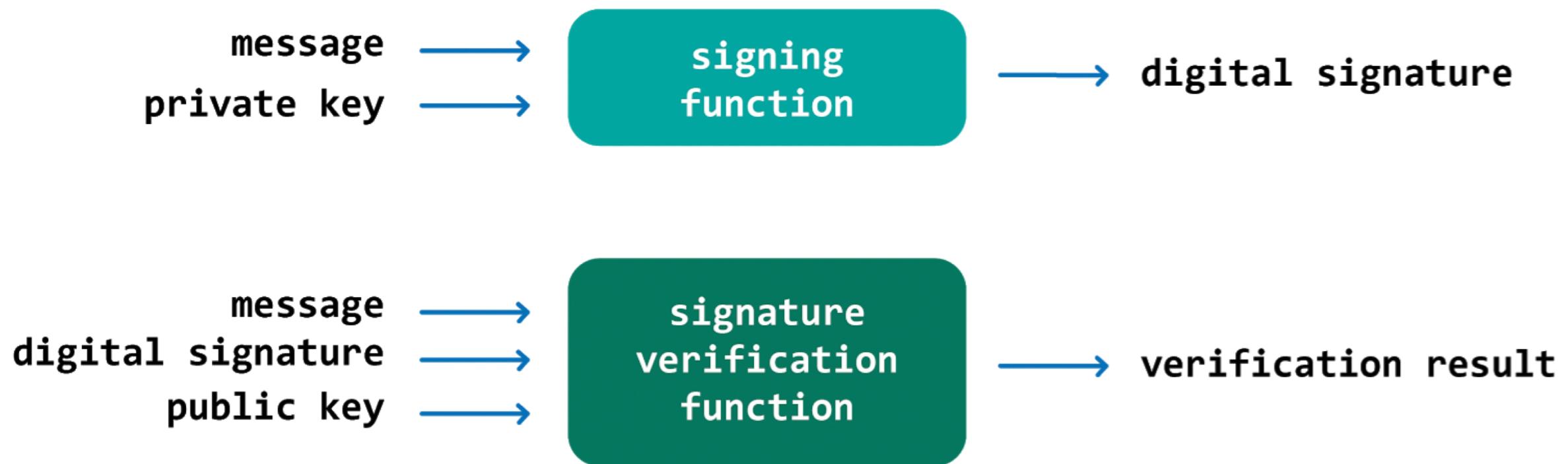
Життєвий цикл сертифіката

1. Створення запиту до центру сертифікації на випуск сертифіката відкритого ключа та верифікація ідентифікаційних даних користувача.
2. Випуск сертифіката відповідно до даних, зазначених у запиті, та чинної політики сертифікації
3. Розповсюдження сертифікату серед учасників інформаційної системи.
4. Зберігання та видача сертифіката на запит користувачів та власників сертифікатів.
5. Призупинення та відновлення дії сертифіката.
6. Оновлення інформації, що міститься в сертифікаті, та ключової пари.
7. Від cliкання сертифіката на запит власника або уповноваженого органу.
8. Закінчення терміну дії сертифіката та перевипуск за потреби.

Проблеми Інфраструктури відкритих ключів

- Складнощі швидкого оповіщення про компрометацію ключа
- Може бути випущено кілька сертифікатів на те саме ім'я у різних кореневих ЦС
- Складний процес оновлення сертифікатів
- Існування різних стандартів електронного підпису
- Центр системи завжди є точкою атаки
- Управління ідентифікатором перебуває у руках централізованої організації

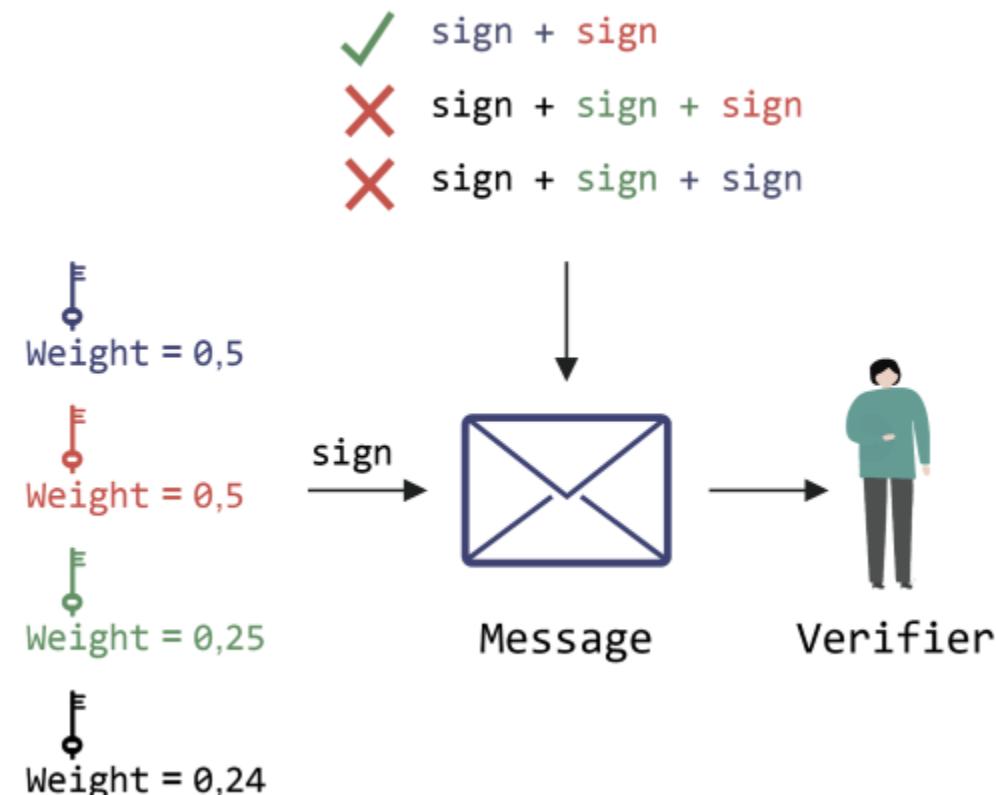
Цифровий підпис



Нетрадиційні різновиди цифрових підписів

- Одноразовий підпис
- Пороговий підпис
- Груповий підпис
- Кільцевий підпис
- Сліпий підпис

Нетрадиційні різновиди цифрових підписів. Пороговий підпис



Нетрадиційні різновиди цифрових підписів. Груповий підпис

