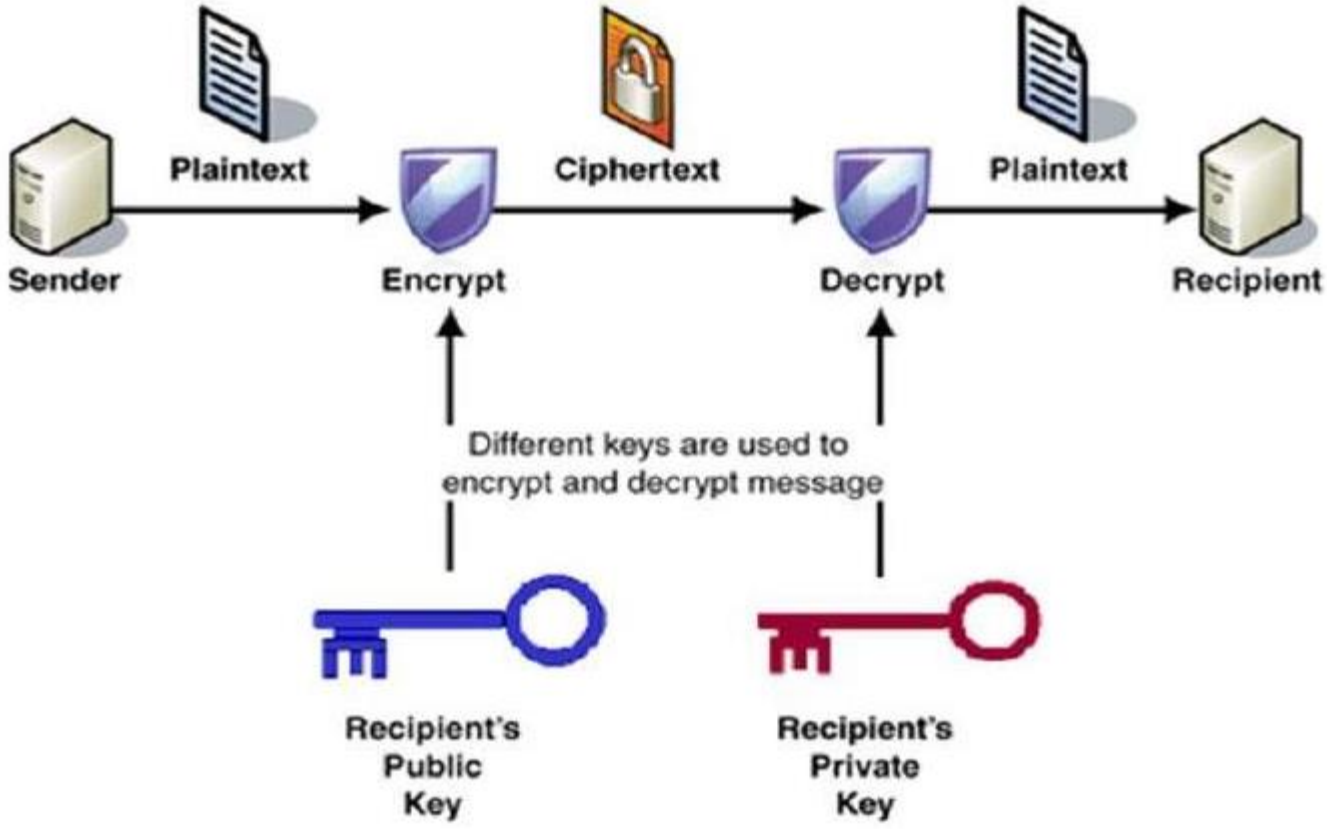
Прикладна криптологія

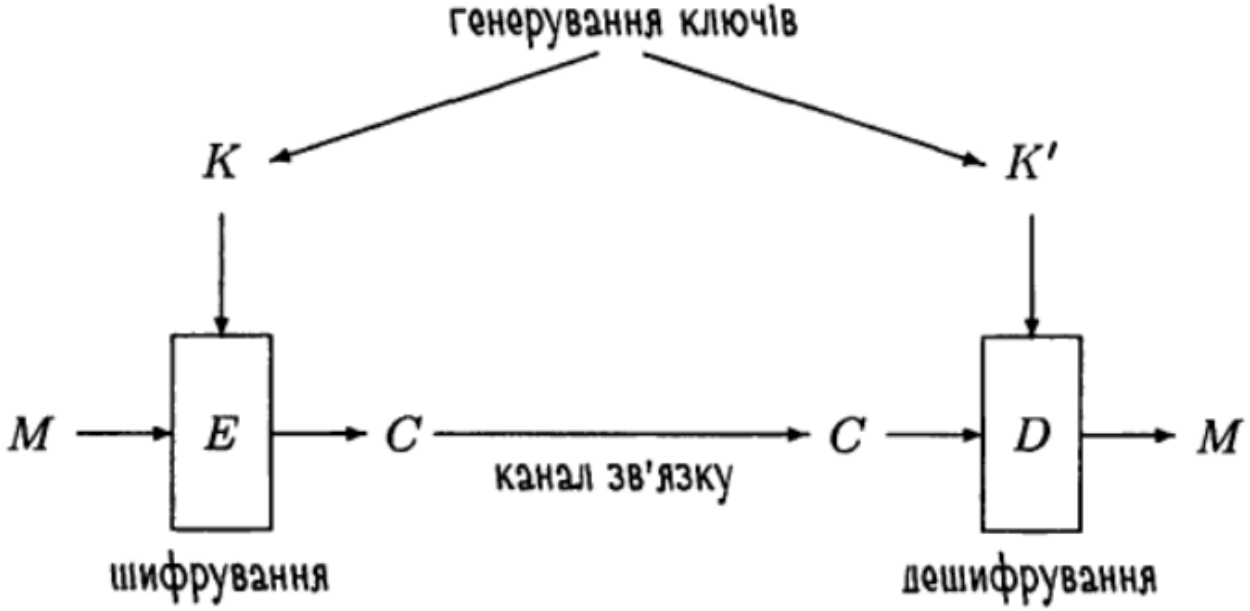
Асиметричні криптосистеми

Криптосистеми з відкритим ключем

1976 рік відкрив сучасний етап у криптографії. Для новітньої криптографії характерною рисою є поява принципово нових криптографічних задач, а також принципово нових розв'язків задач класичних. Тому часто говорять про революцію у галузі криптографії. Поступ, що відбувся у 1976 році, пов'язаний з іменами американських математиків Вайтфілда Діффі та Мартіна Гелмана, а також Ральфа Меркле, які розвинули ідеологію відкритого ключа.

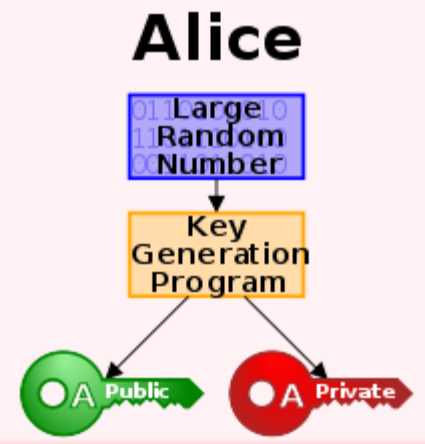


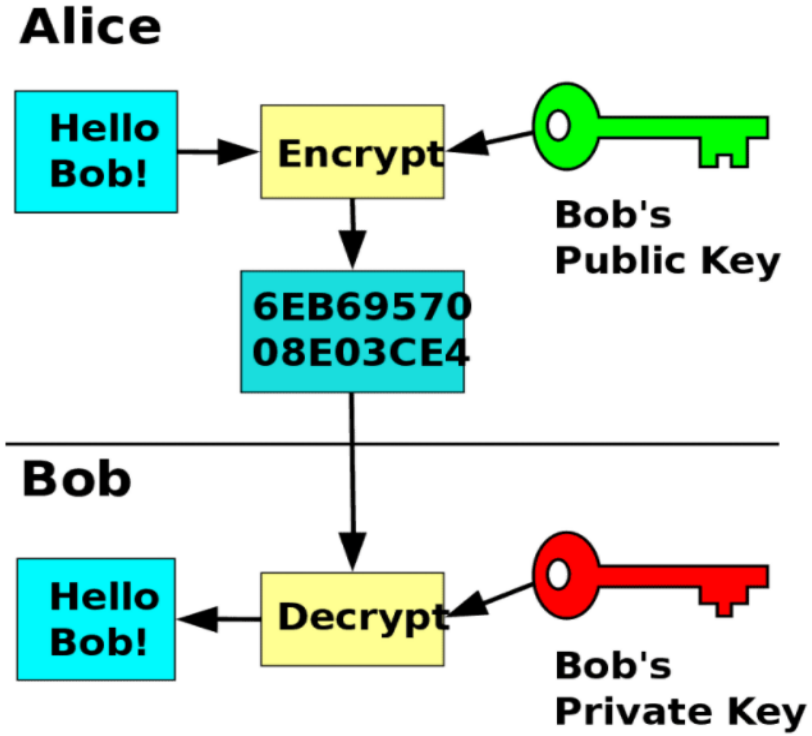
Коцепция



- Алгоритм генерування ключів. Це поліномний ймовірнісний алгоритм, який на вході k, де $k \in N$ — записаний в унарній системі параметр надійності, видає випадкову пару $K, K' \in K$. K називається *відкритим ключем* і використовується для шифрування, а K' називається таємним ключем і використовується для дешифрування.
- Поліномний детермінований алгоритм шифрування E, який отримує на вхід повідомлення M і відкритий ключ K, а видає криптотекст C, що записуємо як $C = E_к(M)$.
- Поліномний детермінований алгоритм дешифрування D, який отримує на вхід криптотекст C і таємний ключ K', а видає відкритий текст C, що записуємо як $M = Dк'(C)$.
- Якщо пара (K, K') породжена алгоритмом генерування ключів, то з $C = E_K(M)$ випливає $M = D_{K'}(C)$ для будь-якого відкритого тексту M.
- Немає (чи, принаймні, невідомо) жодного ефективного алгоритму, який за відомими $C = E_K(M)$ і K знаходив би M.

Концепція





Нова асиметрична схема дозволяє влаштувати довірливе спілкування в мережі оптимальнішим чином. Кожен абонент, власноручно або через менеджера мережі, генерує власну пару ключів *(K, K')*.

Аліса стає власником пари ключів (K_A, K'_A), Боб — $(K_Б, K'_Б)$ і т.д. Кожен абонент свій приватний ключ зберігає в таємниці, в той час як список всіх відкритих ключів $(K_A, K_Б, K_B, K_Г, ...)$ є у загальному доступі. Коли Боб хоче послати Алісі повідомлення M, він посилає їй криптотекст $C = Eк_A(M)$. Оскільки тільки Аліса знає таємний ключ K'_A, лише вона здатна дешифрувати C.

Таким чином, таємницю листування збережено з використанням лише n пар відкритого та таємного ключів, на противагу до необхідних раніше $n(n — 1)/2$ ключів.

RSA (Rivest, Shamir, Adleman)

Запропонована 1977 року система RSA є чи не найпопулярнішою криптосистемою з відкритим ключем. Назва системи утворена з перших літер імен її винахідників — Рональда Райвеста, Аді Шаміра та Леопарда Адлемана.

Генерування ключів. Вибирають два досить великі прості числа p і q. Для їх добутку $n = pq$ значення функції Ойлера дорівнює $\phi(n) = (p - 1)(q - 1) = n – p – q + 1$. Далі випадковим чином вибирають елемент e, що не перевищує значення $\phi(n)$ і взаємно простий з ним. Іншими словами, e є випадковим елементом із множини $Z^*_{\phi(n)}$. Для e за алгоритмом Евкліда знаходить елемент d, обернений до e в $Z^*_{\phi(n)}$, тобто такий, що $d < \phi(n)$ і

$$ed \equiv 1 (\text{mod } \phi(n)) \quad (1)$$

Як результат покладають:

***Відкритий ключ*:** e, n.

***Таємний ключ*:** d.

Шифрування відбувається блоками. Для цього повідомлення записують у цифровій формі і розбивають на блоки так, що кожен блок позначає число, яке не перевищує n. Скажімо, якщо блок записаний у вигляді двійкового слова довжини m, то повинна виконуватись нерівність $2^m < n$. Блок M розглядається як елемент кільця Z_n і як такий, може підноситись до степеня за модулем n.

$$E(M) = M^e mod\ n.$$

Дешифрування:

$$D(C) = C^d mod\ n.$$

Піднесення до степеня за модулем *n*

Задано: $x \in Z_n,\ d \in N$

Обчислити: $x^d \bmod n$.

Завжди можна вважати, що $d < n$. Інакше можна скористатися теоремою Ойлера, щоб понизити показник. Якщо ми використаємо для розв'язання цієї задачі прямолінійну програму (з множенням в кільці Z_n), то отримаємо експоненційний алгоритм:

$z_1 = x*x$

$z_2 = z_1 *x$

...

$z_{d-1} = z_{d-2} * x$

Бінарний метод

Подамо показник d у двійковій системі числення: $d = (d_i \ldots d_1\ d_0)_2$ де $d_i \in \{0,1\}$ і $d = \sum_{i=0}^{l} d_i 2^i$ Покладемо $z_0 = 1$. Тоді i-та команда задається так:

$$z_i = \begin{cases} z_{i-1} * z_{i-1}, \text{де } d_{l+1-i} = 0 \\ z_{i-1} * z_{i-1} * x, \text{де } d_{l+1-i} = 1 \end{cases}$$

Всього команд l+1. Результат виконання останньої:

$$(\ldots((x^{d_l})^2 x^{d_{l-1}})^2 x^{d_{l-2}} \ldots)^2 x^{d_0} = x^{d_l 2^l + d_{l-1} 2^{l-1} + \ldots + d_0 2^0} = x^d$$

Коректність, ефективність, надійність

Коректність: Слід пересвідчитись, що $D(E(M)) = M$ для довільного повідомлення M.

Твердження 2.2. *Нехай $n = pq$ є добутком двох різних простих чисел. Якщо $ed \equiv 1 \pmod{\phi(n)}$, то для всіх $x \in \mathbb{Z}_n$*

$$x^{ed} \equiv x \pmod{n}.$$

Ефективність: Алгоритм генерування ключів використовує процедуру породження простих чисел і розширений алгоритм Евкліда для обчислення НСД(e, $\phi(n)$) і $d = e^{-1} mod\ \phi(n)$. В алгоритмах шифрування та дешифрування піднесення до степеня виконується за допомогою бінарого методу.

Надійність: Щоб криптосистема вважалась надійною, необхідно щоб задача визначення повідомлення за криптотекстом і відкритим ключем була важкою. Задача розкриття RSA є задачею добування із заданого числа кореня e-го степеня за модулем $n=pq$. На сьогоднішній момент для цієї задачі невідомо ніякого ефективного алгоритму. Однак не доведено, що такого алгоритму не існує.

Розкриття RSA
Задано: e, n, y, де $n = pq$ і НСД$(e, \phi(n)) = 1$.
Знайти: x таке, що $x^e \equiv y \pmod{n}$.

Знаходження таємного ключа для RSA

Будь-яку асиметричну криптосистему можна зламати, вказавши ефективний спосіб визначення таємного ключа за відкритим ключем. У нашому випадку це означає, що розкриття RSA зводиться до задачі:

- *Задано:* e, n, де $n = pq$ і НСД $(e, \phi(n)) = 1$.
- *Знайти:* d таке, що $x^{ed} = x \pmod{n}$ для всіх x.

З алгоритму генерування ключів безпосередньо випливає, що остання задача зводиться до обчислення значення функції Ойлера $\phi(n)$:

- *Задано*: $n = pq$, де p та q непарні прості.
- *Обчислити*: $\phi(n)$.

Слід зазначити, що співмножники p і q не входять в умову задачі. Однак якщо вони відомі, то $\phi(n)$ легко обчислюється за формулою $\phi(pq) = (p - 1)(q - 1)$. Таким чином обчислення функції Ойлера від аргументів виду $n = pq$ зводиться до факторизації таких чисел. спроба факторизувати модуль $n = pq$ є найочевиднішим шляхом до розкриття RSA. При генеруванні ключа, p і q рекомендується вибирати із приблизно сотнею десяткових цифр кожне. Вибір таких чисел повинен бути справді випадковим, щоб уникнути можливої факторизації якимось із вузькоспеціальних методів

Має місце й обернене зведення. Припустимо, що для числа $n = pq$ відоме значення $\phi(n)$. Зауважимо, що

$\phi(n) = n - p - q + 1$. Тому співмножники p і q визначаються із системи

$$\begin{cases} pq = n \\ p + q = n + 1 - \phi(n), \end{cases}$$

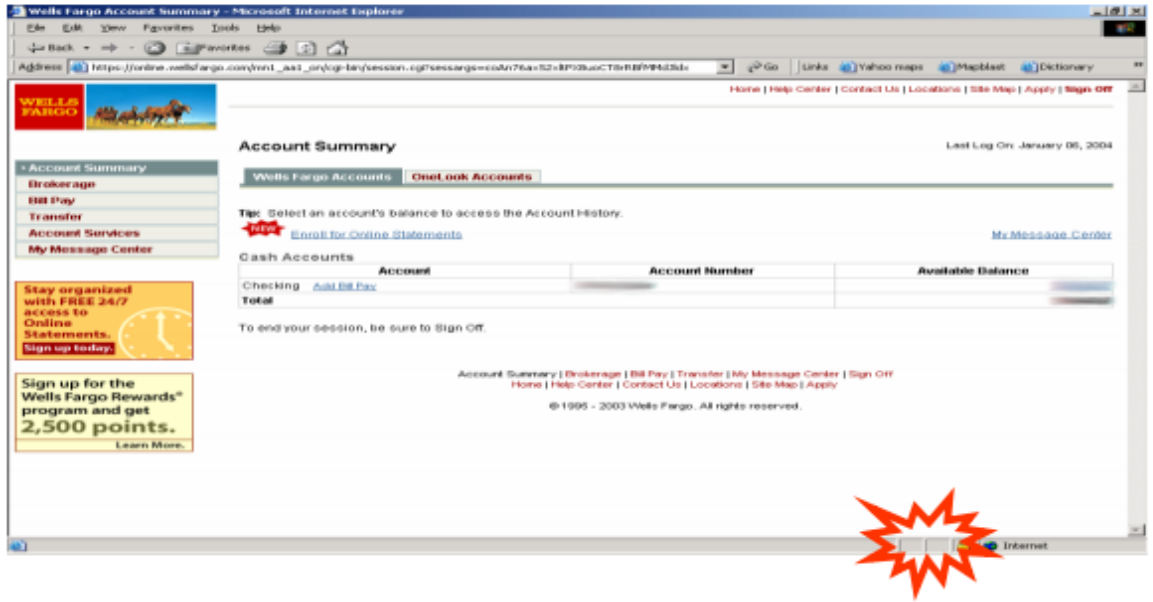
тобто є розв’язком квадратного рівняння

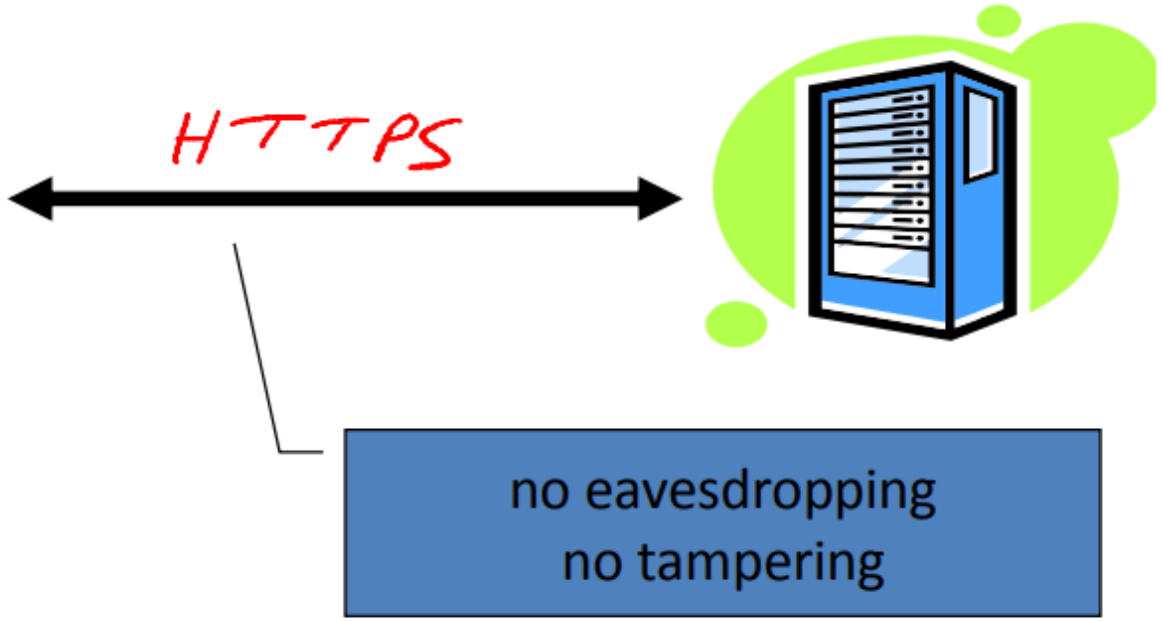
$$X^2 - X(n + 1 - \phi(n)) + n = 0.$$

Застосування криптографічних систем

Шифрування інформаційного потоку

- **web traffic: HTTPS (RSA, AES);**
- **wireless traffic: 802.11, WPA2 (and WEP), GSM, Bluetooth (RC4, A5)**





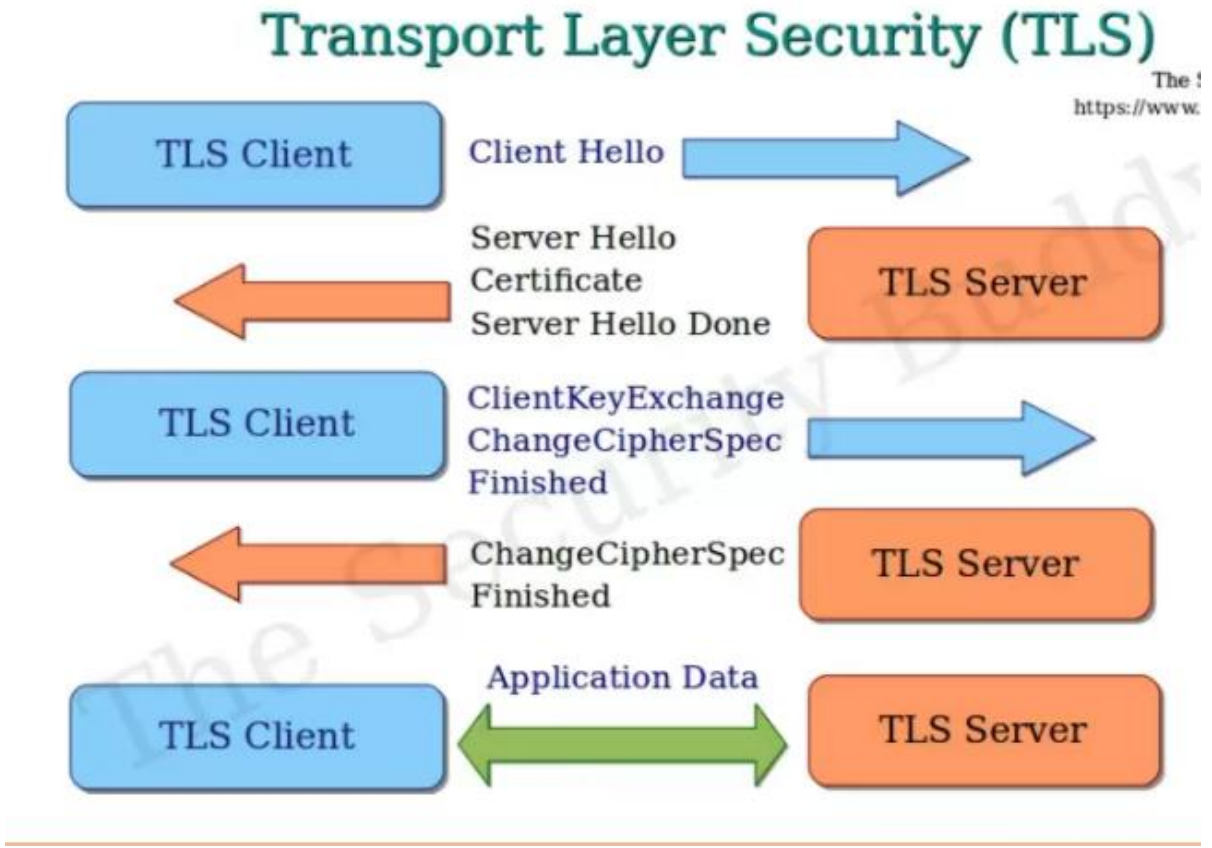
Криптографічний протокол SSL/ TLS

Протокол — це послідовність кроків, які роблять дві або більше сторін для спільного вирішення завдання.

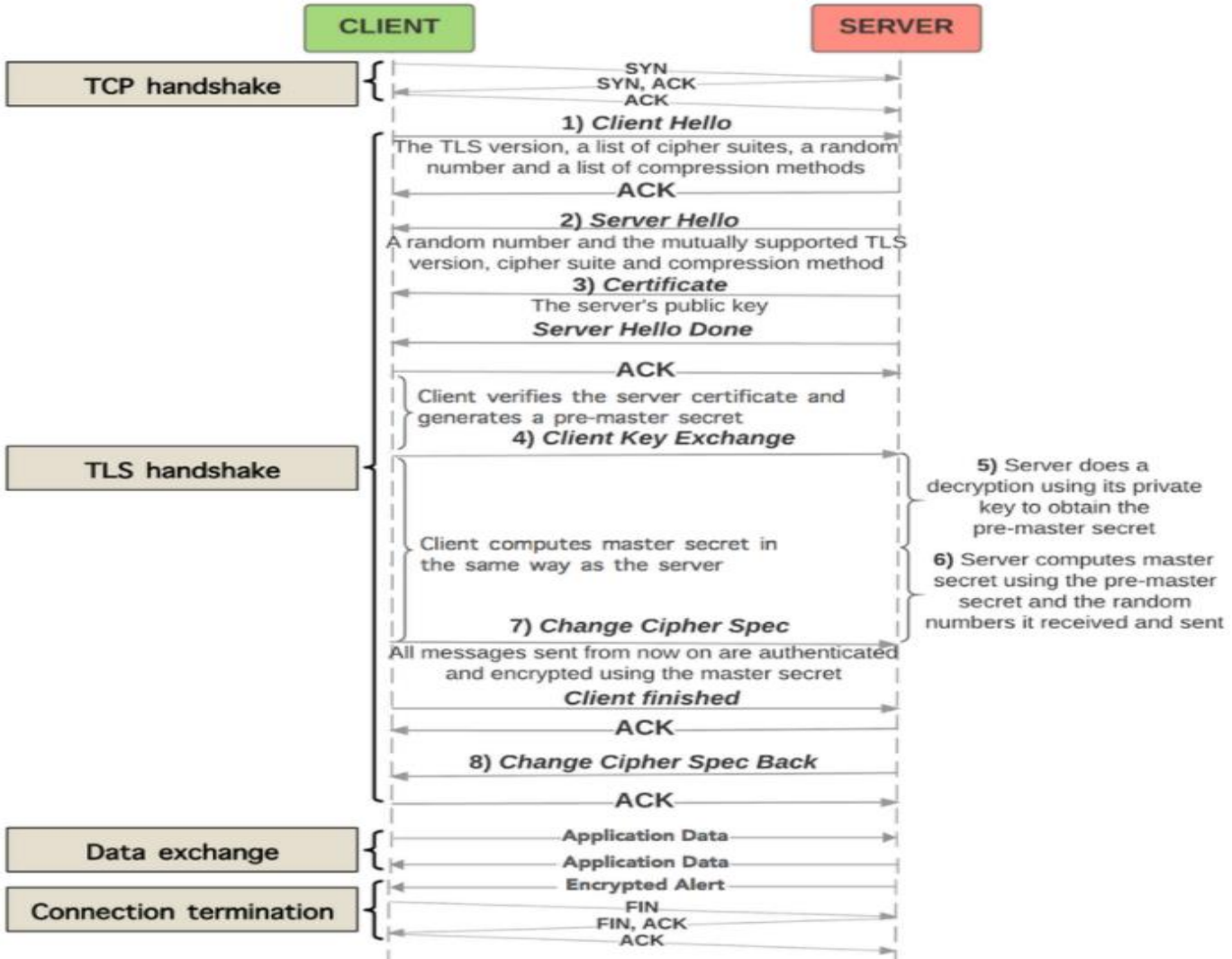
Криптографічним протоколом називається такий, в основі якого лежить криптографічний алгоритм.

Дві основні частини SSL/TLS:

- Handshake Protocol: Встановлення спільного секретного ключа за допомогою криптографії з публічним ключем;
- Record Layer: Передача даних за допомогою спільного секретного ключа, що Забезпечує конфіденційність та цілісність



TLS Handshake



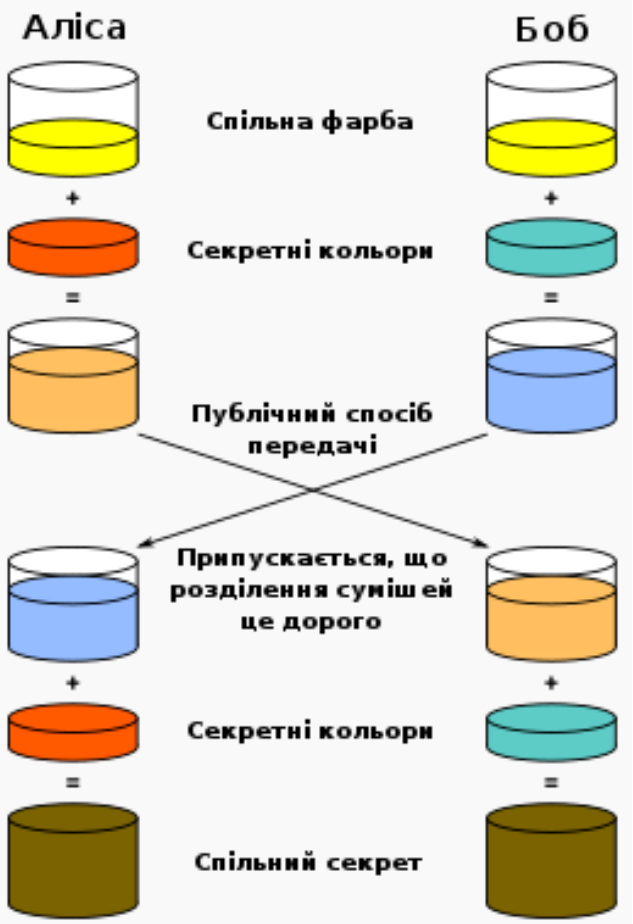
Протокол обміну ключем Діффі-Геллмана

Diffie–Hellman key exchange — це метод обміну криптографічними ключами. Один з перших практичних прикладів узгодження ключа, що дозволяє двом учасникам, що не мають жодних попередніх даних один про одного, отримати спільний секретний ключ із використанням незахищеного каналу зв'язку. Цей ключ можна використати для шифрування наступних сеансів зв'язку, що використовують шифр з симетричним ключем.

- Аліса вибирає велике просте число p та первісний корінь g за модулем p ($g^{\varphi(p)} \equiv 1 \; mod \; p$), і відкрито відправляє Бобові.
- Аліса вибирає випадкове число a в межах від 1 до p-1, а Боб – випадкове число b в тих же межах.
- Аліса обчислює $g^a mod\, p$ і відправляє це значення Бобові, а Боб обчислює $g^b mod\, p$ і відправляє Алісі.
- І Аліса, і Боб обчислюють одне і теж число

$$(g^b)^a mod\, p = (g^a)^b mod\, p = g^{ab} mod\, p.$$

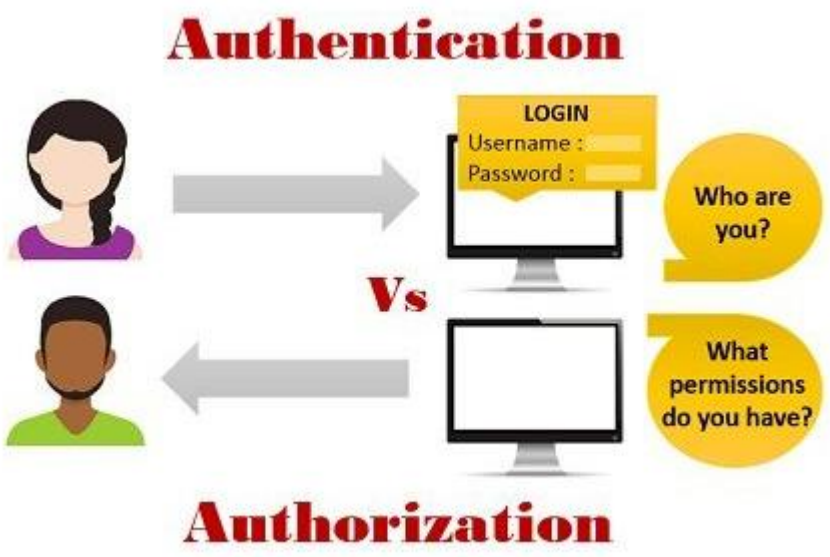
Однак, базовий варіант протоколу узгодження ключа анонімний, тут відсутня можливість автентифікації абонентів. Таким чином, протокол вразливий для атаки «людина посередині».



Схематична ілюстрація протоколу на прикладі змішування фарб

Клас	Протокол узгодження ключів
Структура даних	Швидкодія та криптографічна стійкість залежать від обраного простору (циклічної групи)

Автентифікація та авторизація



Цифровий сертифікат

Цифровий сертифікат — цифровий документ, який є одним із засобів підтвердження відкритого (публічного) ключа приналежності його власникові.

Існує дві моделі організації інфраструктури сертифікатів:

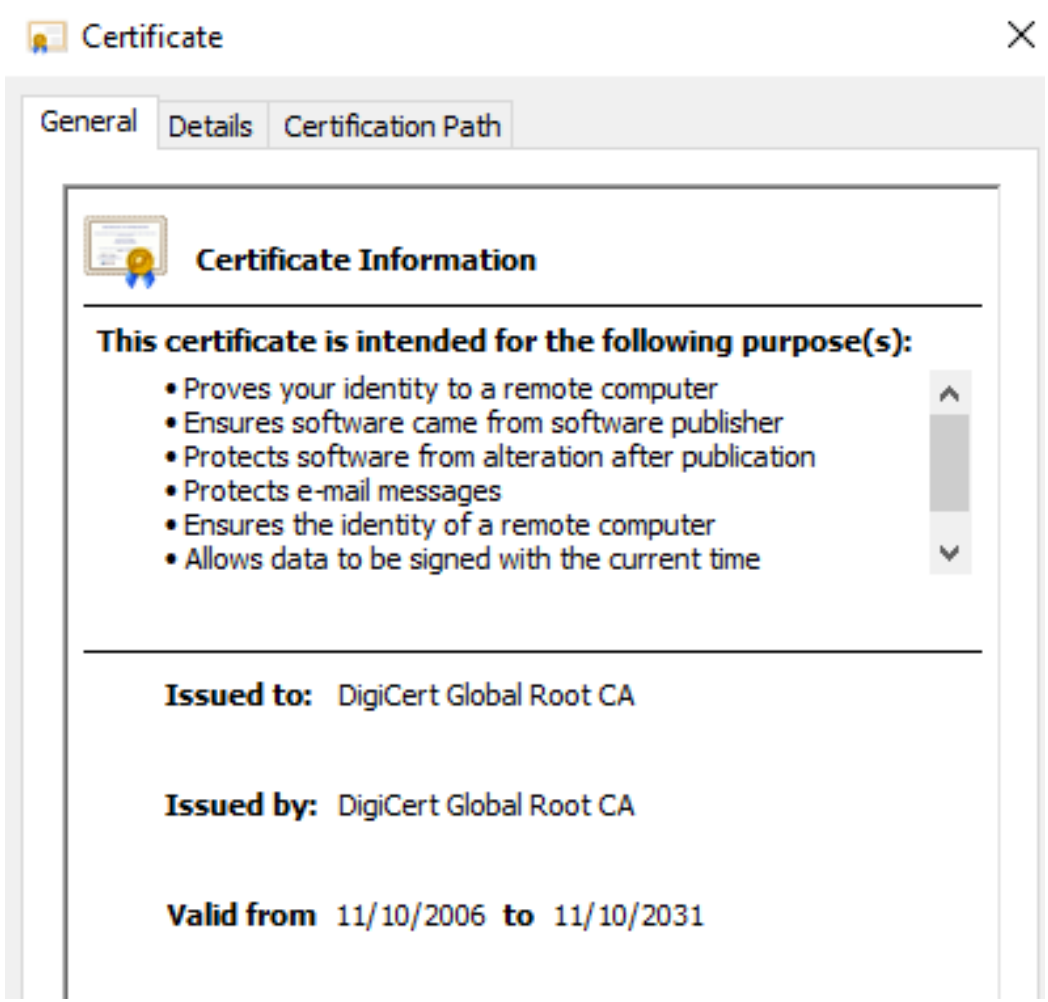
- централізована або інфраструктура відкритих ключів (англ. PKI) — в цій моделі всі користувачі довіряють тільки тим сертифікатам, які підписані кореневими центрами сертифікації;
- децентралізована — кожен користувач самостійно обирає, яким сертифікатам довіряти та в якій ступень.

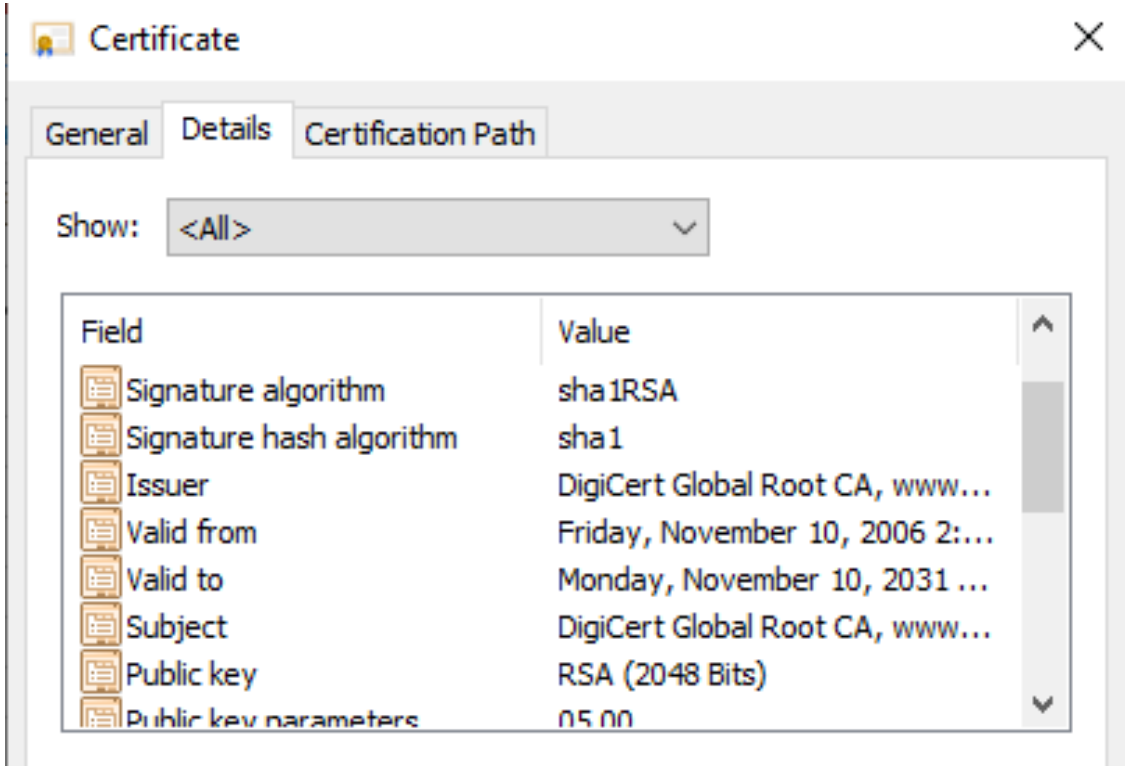
Найчастіше файл сертифіката являє собою файл стандарту X.509 в CER або PEM форматі (*.cer), який містить відкритий ключ та ідентифікаційні дані власника ключа та підписаний цифровим підписом центра сертифікації.

Сертифікат містить:

- серійний номер сертифіката;
- назва алгоритму цифрового підпису;
- назва центра сертифікації, що підтвердив підпис власника;
- термін дії сертифікату з ... по ... ;
- ім'я користувача, якому належить сертифікат;
- відкритий (публічний) ключ власника сертифіката (ключів може бути декілька);
- об'єктні ідентифікатори алгоритмів, асоційованих з відкритими ключами власника сертифіката;
- електронний цифровий підпис центру сертифікації вищенаведених даних. Всі дані, які й власно утворюють сертифікат, отримують цифровій відбиток, якій відбивається в сертифікаті;
- назву видавця (issuer).

Цифровий сертифікат





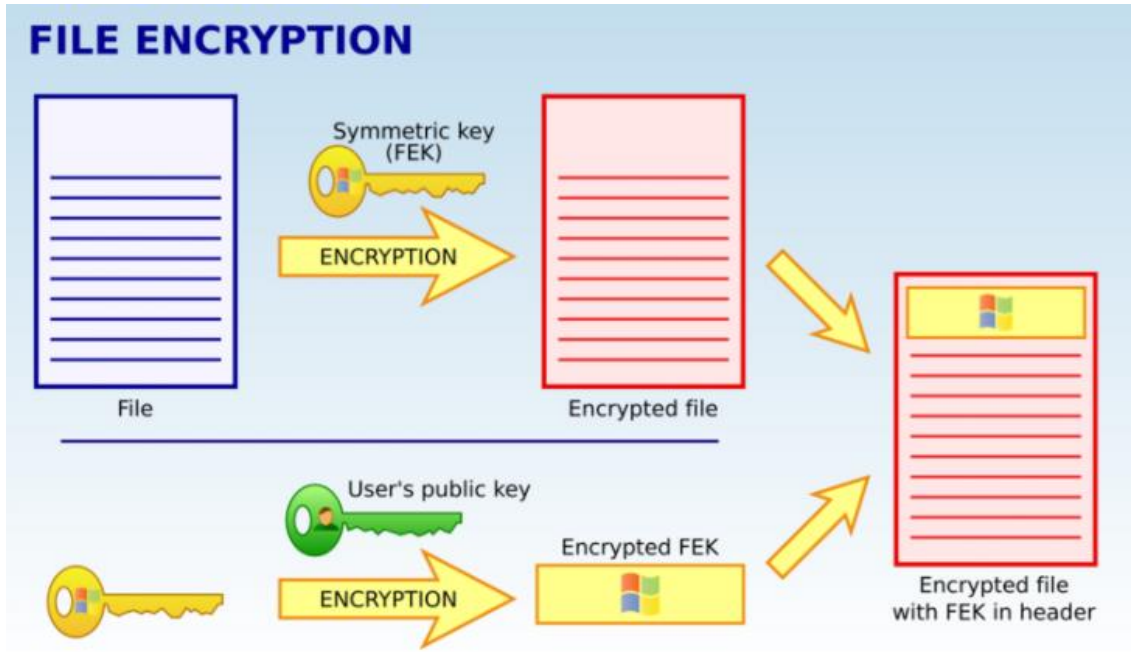
Центр сертифікації

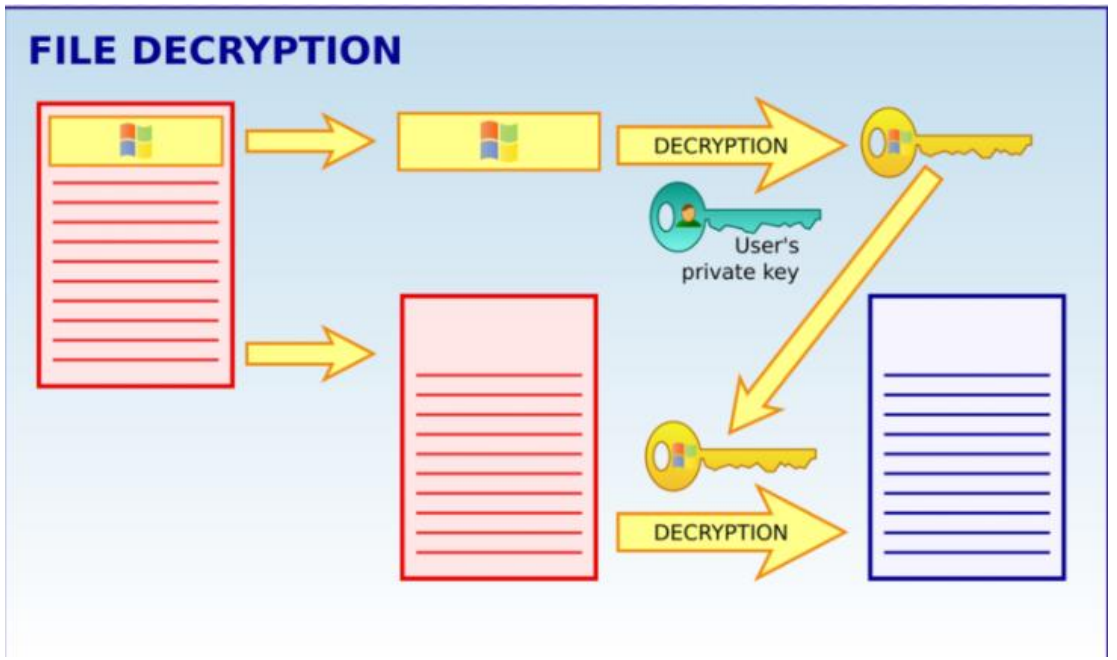
Центр сертифікації (англ. Certification authority, CA) — це організація, яка надає послуги електронного цифрового підпису, зокрема:

- надання у користування засобів електронного цифрового підпису;
- допомога при генерації відкритих та особистих ключів;
- обслуговування сертифікатів ключів:
- формування;
- розповсюдження;
- скасування;
- зберігання;
- блокування;
- надання інформації щодо чинних, скасованих і заблокованих сертифікатів відкритих ключів;
- послуги фіксування часу;
- консультації та інші послуги.

Захист даних на диску

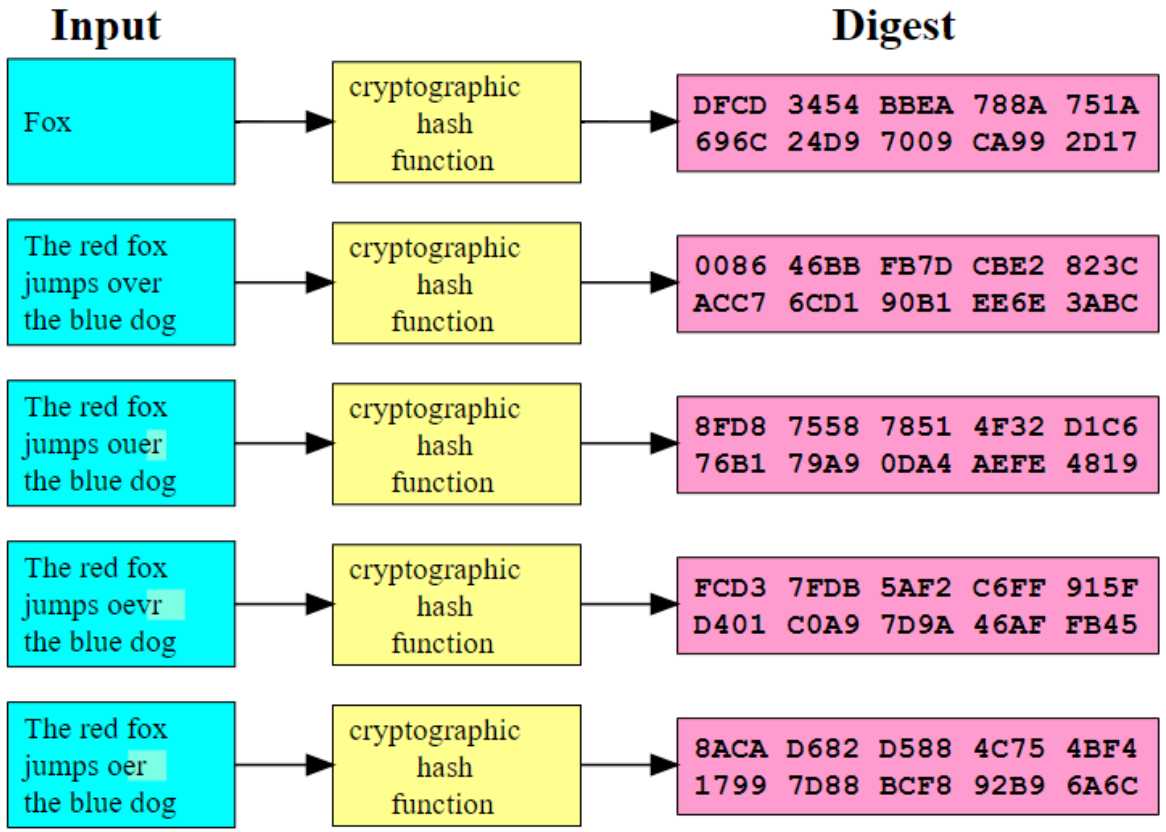
- **Encrypting File System (EFS)** — система шифрування даних, що реалізує шифрування на рівні файлів в операційних системах (Windows).
- **TrueCrypt, VeraCrypt** — програмне забезпечення для шифрування дисків та файлі. Використовує симетричні алгоритми шифрування AES, Twofish, Seprent.





Криптографічні хеш-функції

Криптографічна хеш-функція — це хеш-функція, яка є алгоритмом, що приймає довільний блок даних і повертає рядок встановленого розміру (Message Digest (MD5), Secure Hash Algorithm (SHA-1, SHA-2, SHA-3)).



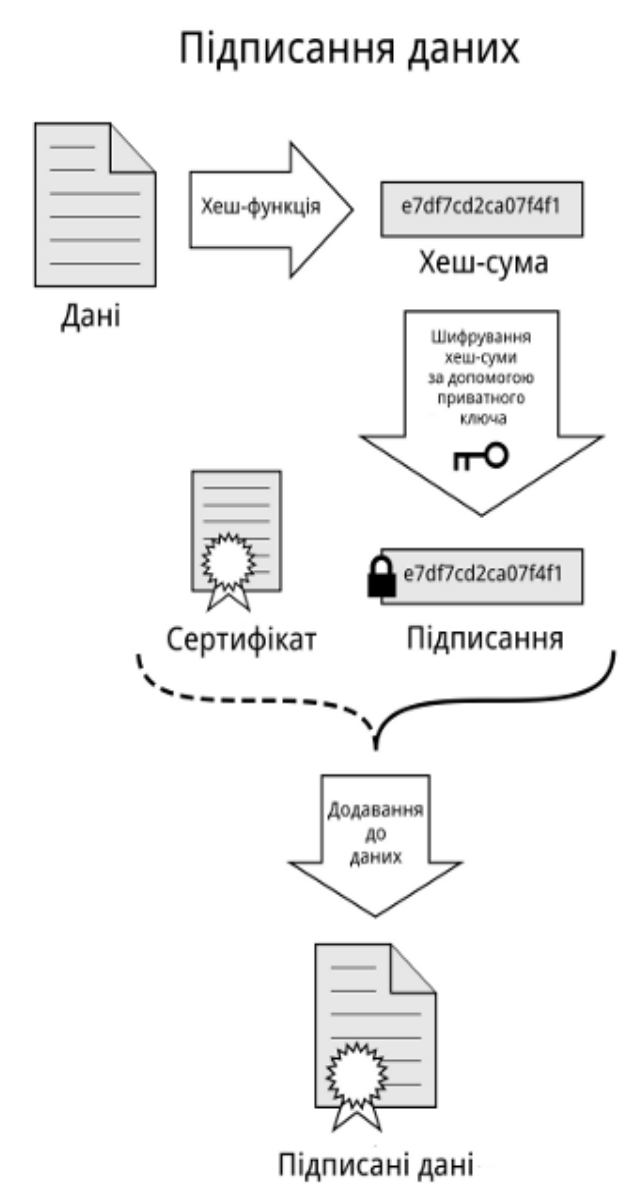
Електронний цифровий підпис

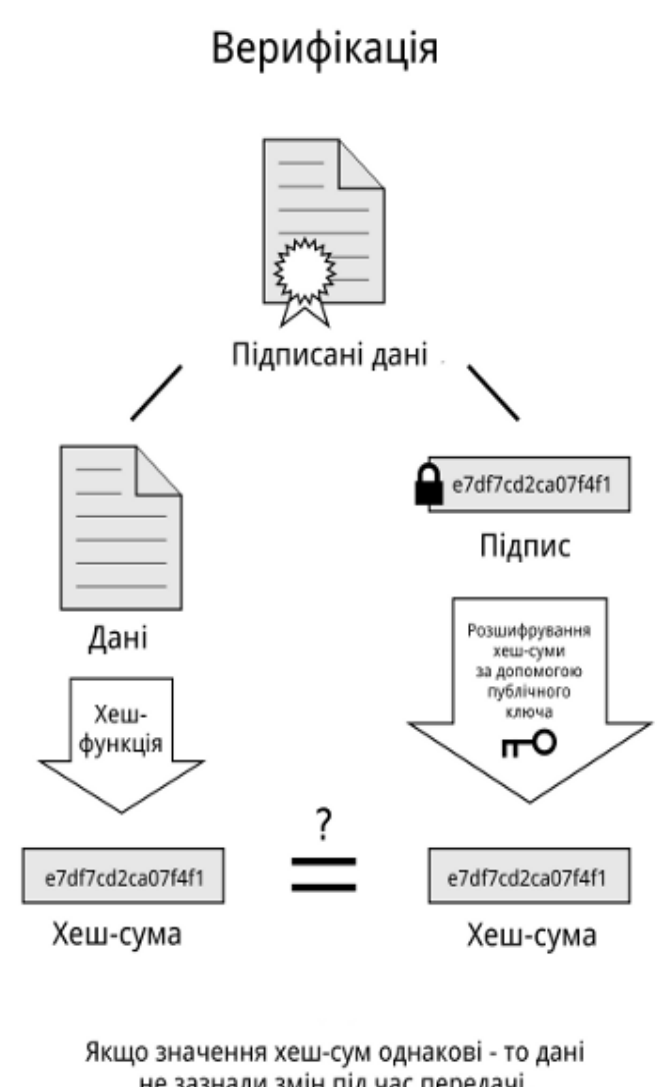
Електронний цифровий підпис (ЕЦП) (англ. digital signature) — вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Електронний цифровий підпис призначений для використання фізичними та юридичними особами — суб'єктами електронного документообігу:

- для аутентифікації підписувача;
- для підтвердження цілісності даних в електронній формі.

Відкритий ключ використовується для перевірки ЕЦП одержуваних документів (файлів). Відкритий ключ працює тільки в парі з приватним ключем. Відкритий ключ міститься в ***Сертифікаті відкритого ключа***, і підтверджує приналежність відкритого ключа ЕЦП певній особі. З метою забезпечення цілісності представлених у Сертифікаті даних він підписується особистим ключем Центру сертифікації ключів.





Цифрова валюта

- **Криптовалюта (Bitcoin) -** принциповою особливістю криптовалют є збереження інформації у блокчейні, де асиметричне шифрування використовується для перевірки повноважень, а інші криптографічні методи — як доказ виконаної роботи
- **Анонімні цифрові гроші**

- Чи можу я витратити «цифрову монету», не знаючи, хто я?

- Як запобігти подвійним витратам?