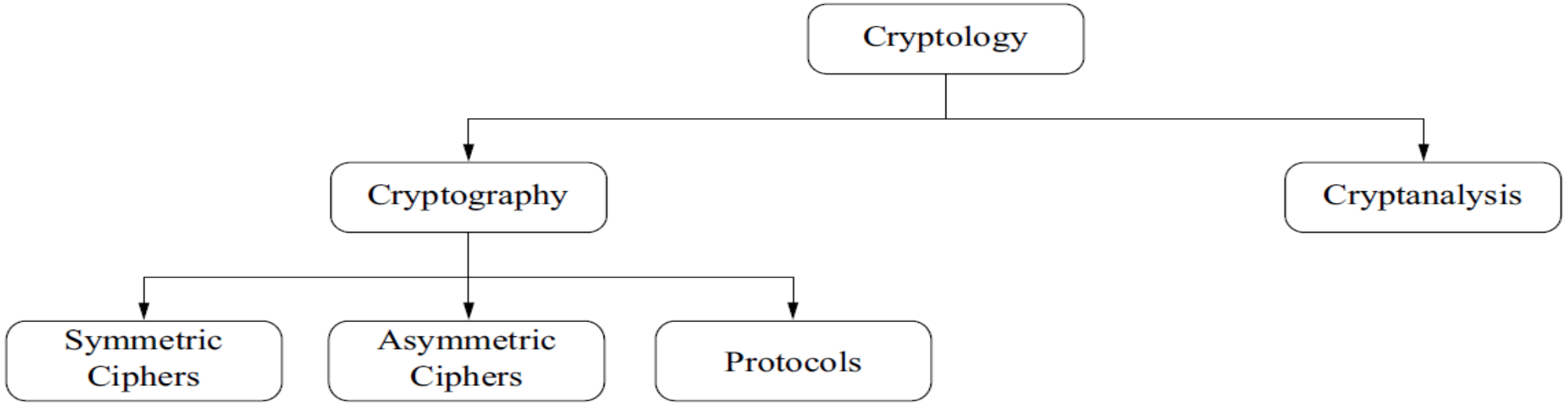
Криптологія

Валерій Миколайович Трушевський

доцент кафедри кібербезпеки ЛНУ ім. І. Франка

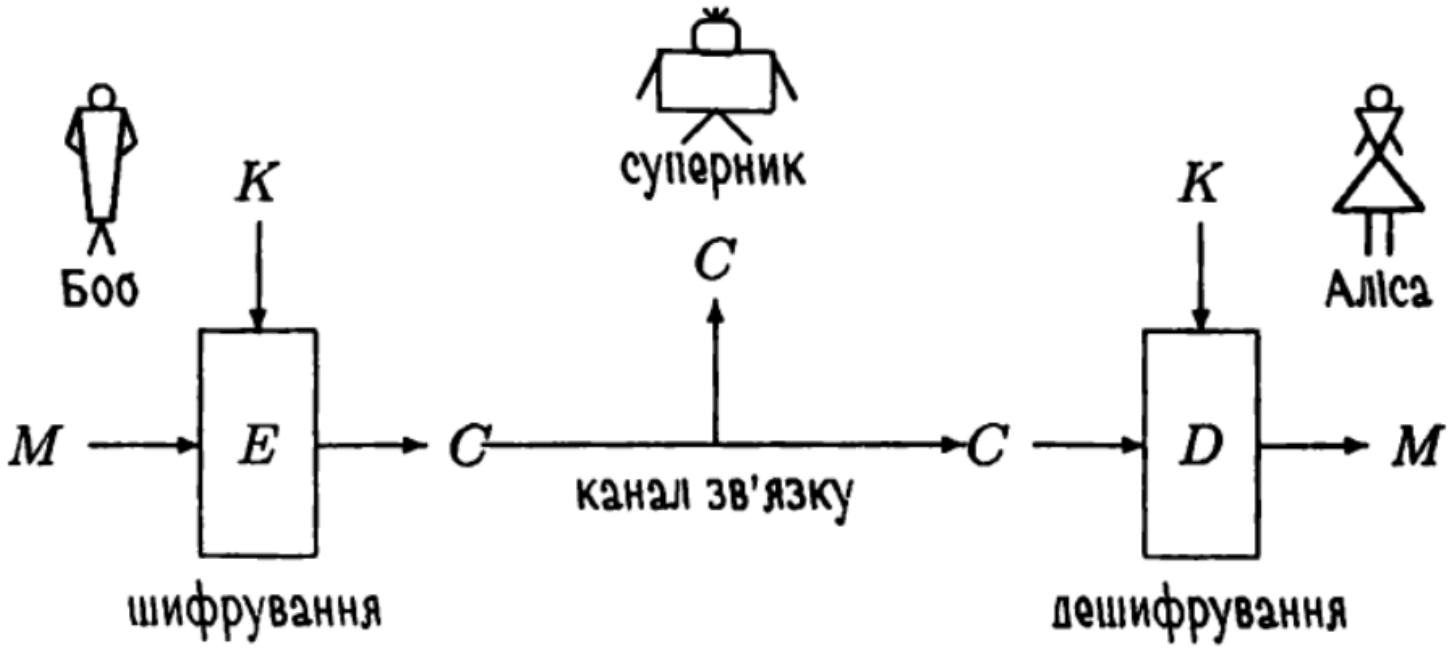
Основні поняття

- **Криптологія (Cryptology) —** це галузь знань, що вивчає тайнопис (криптографію), і методи її розкриття (криптографічний аналіз). Назва криптології пішла від грецької мови (криптос — таємний, логос — наука або слово).
- **Криптографія (Cryptography) —** наука про збереження таємниці тексту.
- **Криптографічний аналіз (Cryptoanalysis) -** наука про проникнення у таємницю захищеного тексту.



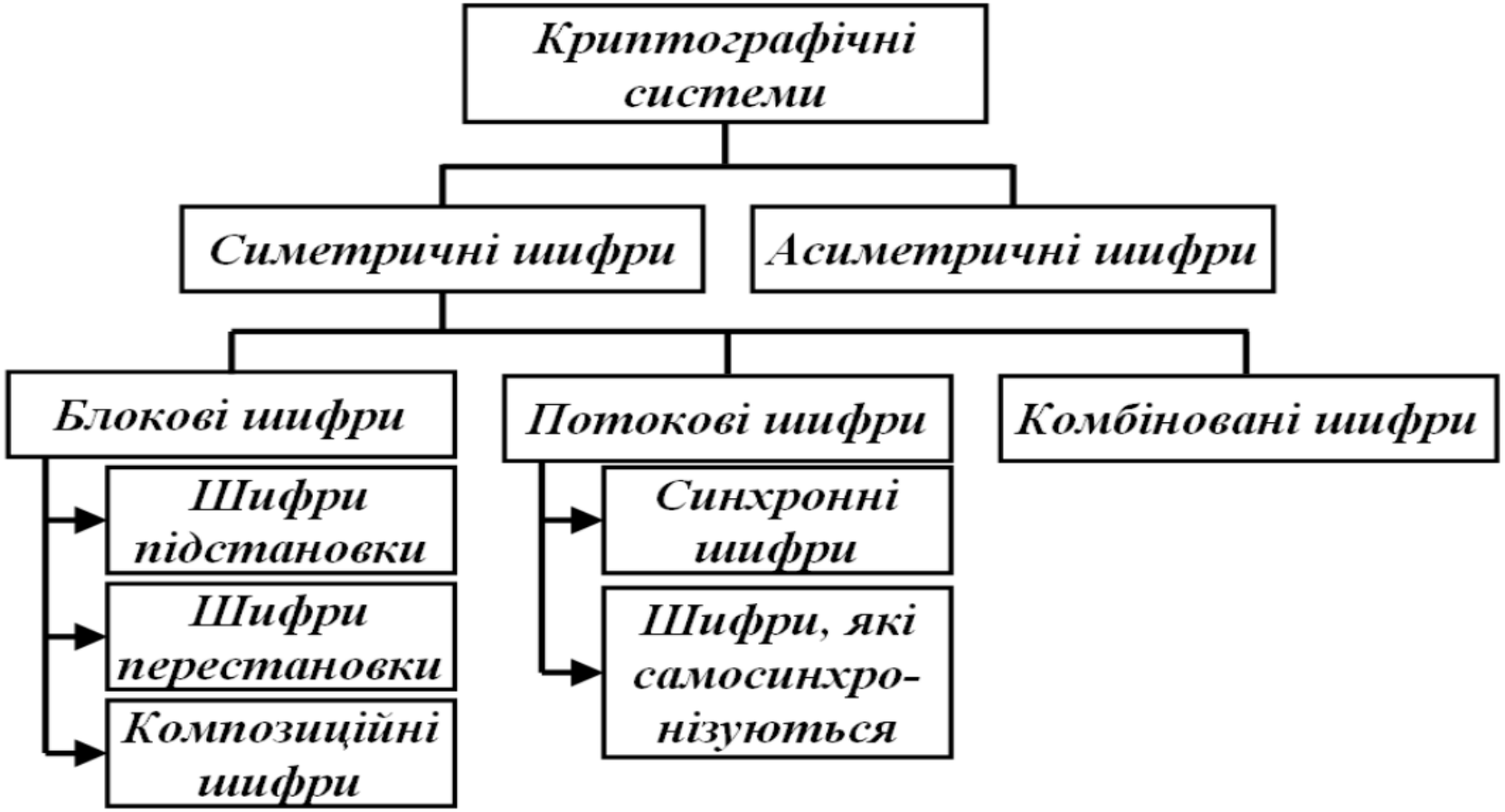
Класична криптографічна схема

- **K (key) –** секретний ключ;
- **E (encryption) –** функція шифрування $C = E_K (M)$;
- **D (decryption) –** функція дешифрування: $M = D_K (C)$;



Симетрична криптосистема

Класифікація методів шифрування

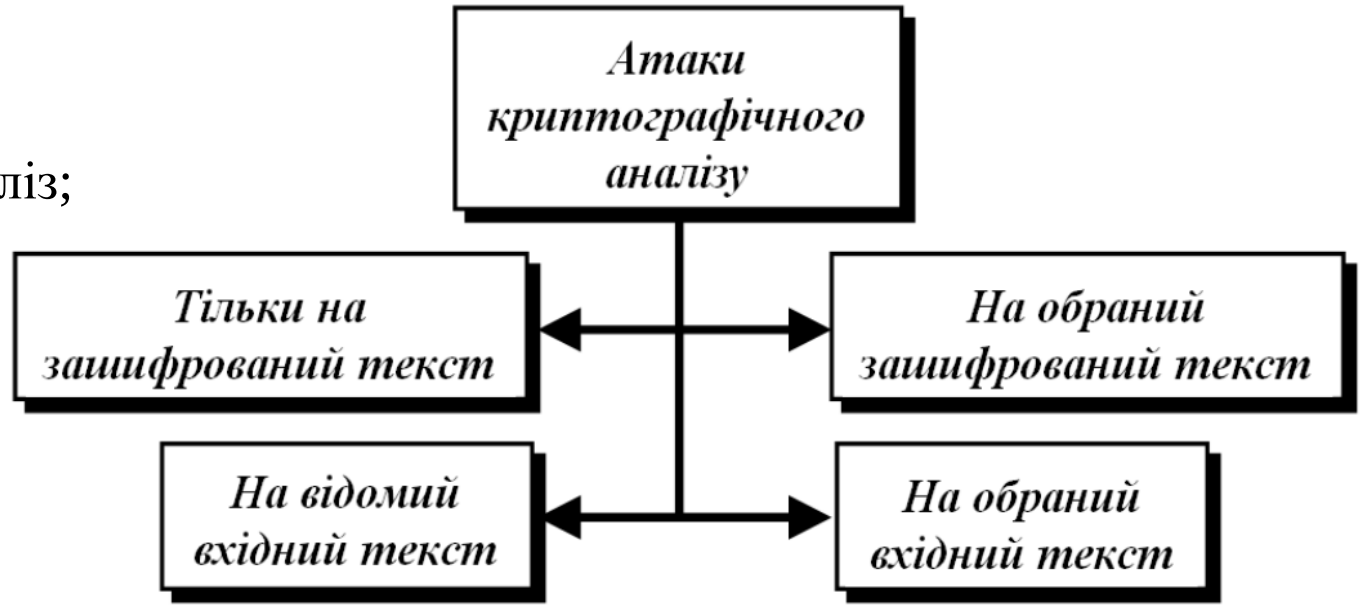


Криптографічна стійкість

- Абсолютно надійний шифр не піддається криптоаналізу;
- Шифр вважається надійним в обчислювальному сенсі, якщо його розкриття хоча в принципі можливе, але навіть на найшвидшемо комп’ютері вимагатиме нереального часу (роки, століття, …), після завершення якого будь-яка таємниця стане неактуальною;
- Принцип Керкгоффза (англ. Kerckhoffs's principle) - стійкість криптографічного алгоритму не має залежати від архітектури алгоритму, а має залежати тільки від ключів.

Криптографічний аналіз

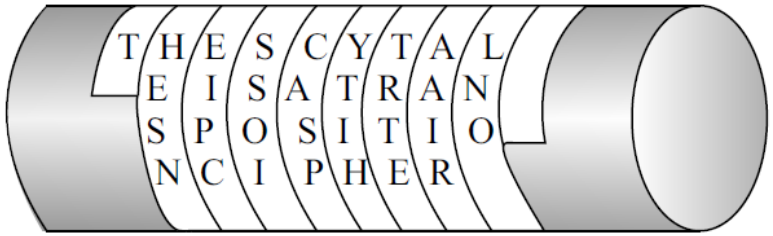
- Атака грубої сили (brute force);
- Статистична атака – частотний криптоаналіз;
- Лінійний криптоаналіз;
- Диференціальний криптоаналіз;
- Атака за зразком.



Симетричні криптосистеми

Шифри перестановки

- **Шифр Скитала -** використовувався спартанцями для військових донесень у V ст. до н.е.



- **Шифр частоколу:** криптографія → игірпорфякта

криптографія

Шифри простої заміни

- **Шифр Ю. Цезаря -** (100 – 44 р. до н.е). Кожна буква алфавіту заміщується циклічним зсувом на 3 позиції вправо: а → г, б → ґ, в → д і т.д.

імперія → лптзулв

- **Частотний криптоаналіз -** У досить довгих текстах кожна буква зустрічається із приблизно однаковою частотою.

пцпспофнпмплпибгпефрптмбвмєоп **охоронумолокозаводупослаблено**

ц	0.134	е	0.043	л	0.028	ч	0.011	ї	0.006
о	0.082	р	0.038	у	0.027	б	0.010	є	0.006
н	0.070	і	0.037	п	0.025	х	0.010	ф	0.005
а	0.070	с	0.036	я	0.021	ц	0.009	ш	0.005
и	0.056	к	0.036	э	0.019	ю	0.009	щ	0.003
т	0.051	м	0.033	ь	0.015	ж	0.008	ґ	0.000
в	0.046	д	0.028	г	0.013	й	0.007		

Шифр Віженера

Шифр Віженера – поліалфавітний шифр який використовує слово в якості ключа. Отримав назву на честь Блеза де Віженера, хоча насправді його винайшов італійський криптограф Джованні Баттіста Белласо (19 ст.)

Шифрування: $C_i = (P_i + K_i) \bmod 33$;

Дешифрування: $C_i = (P_i + 33 - K_i) \bmod 33$

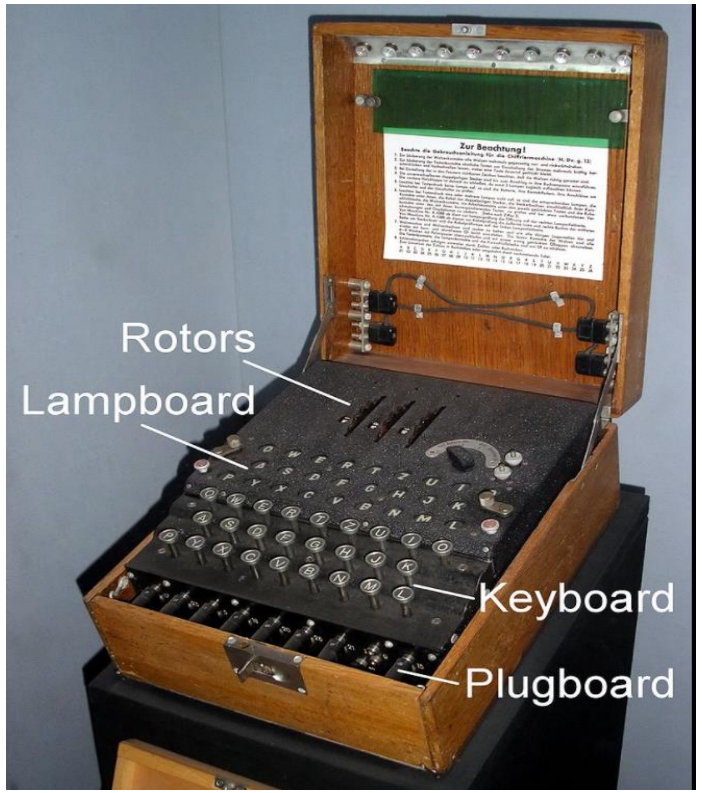
```
  БОРОНІТЬКОРОЛІВНУВІДВОРОГІВ
+ КЛЮЧКЛЮЧКЛЮЧКЛЮЧКЛЮЧКЛЮЧКЛЮ
  ЛАОЇЮЦРФШАОЇЩЦАІҐНЗЯМАОЇНЦА
```

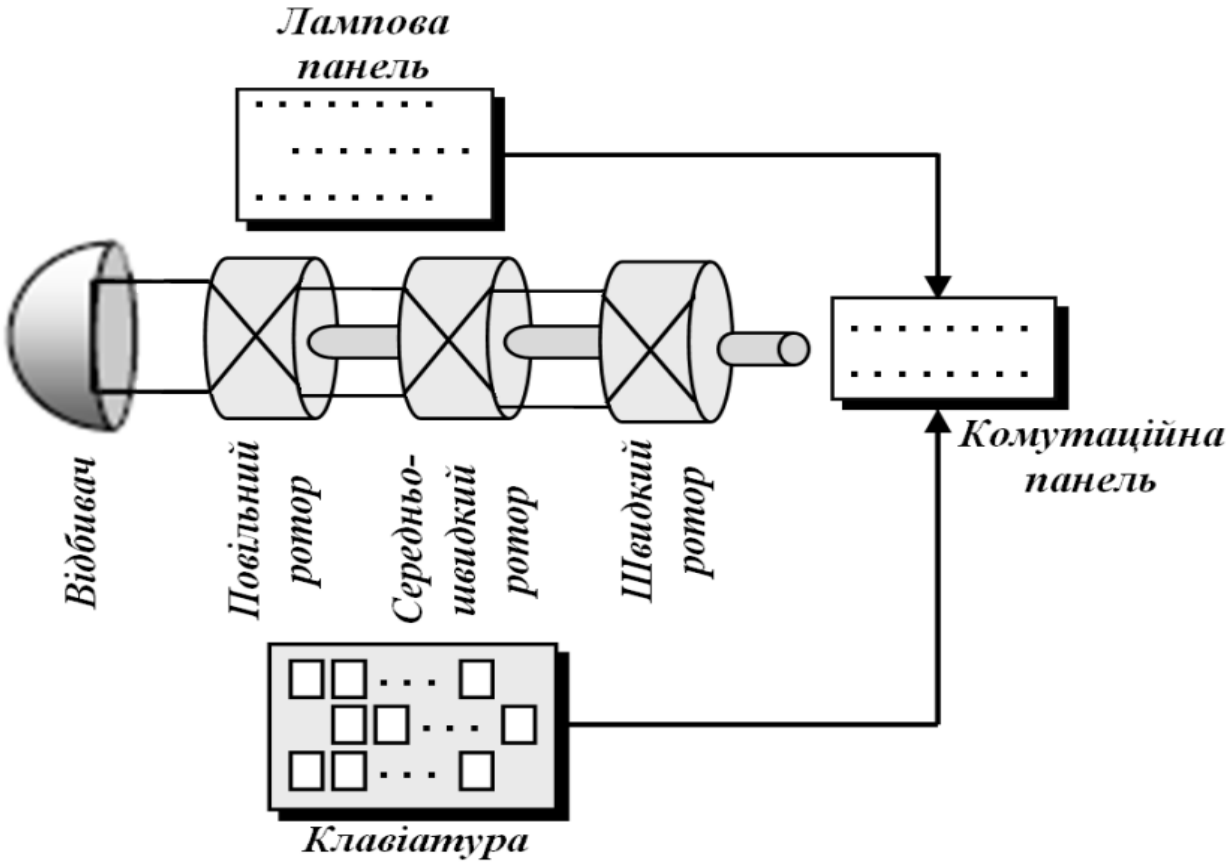
Шифр з автоключем - грунтується на ідеях Віженера та Кардано:

```
  БОРОНІТЬКОРОЛІВНУВІДВОРОГІВ
+ КЛЮЧБОРОНІТЬКОРОЛІВНУВІДВОР
  ЛАОЇОЩЗЛЮЩЗЛЩЩТВДЙЙТХРЮУДЩТ
```

Шифр Enigma

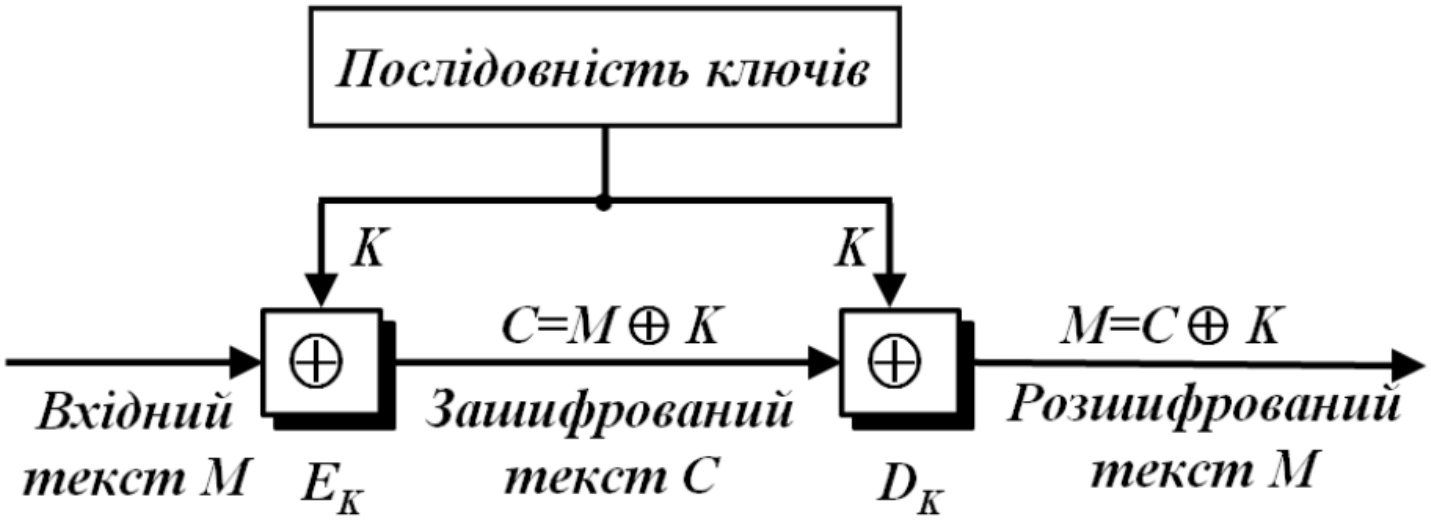
Технічна реалізація шифру була винайдена німецьким інженером Arthur Scherbius на прикінці I-ї світової війни.





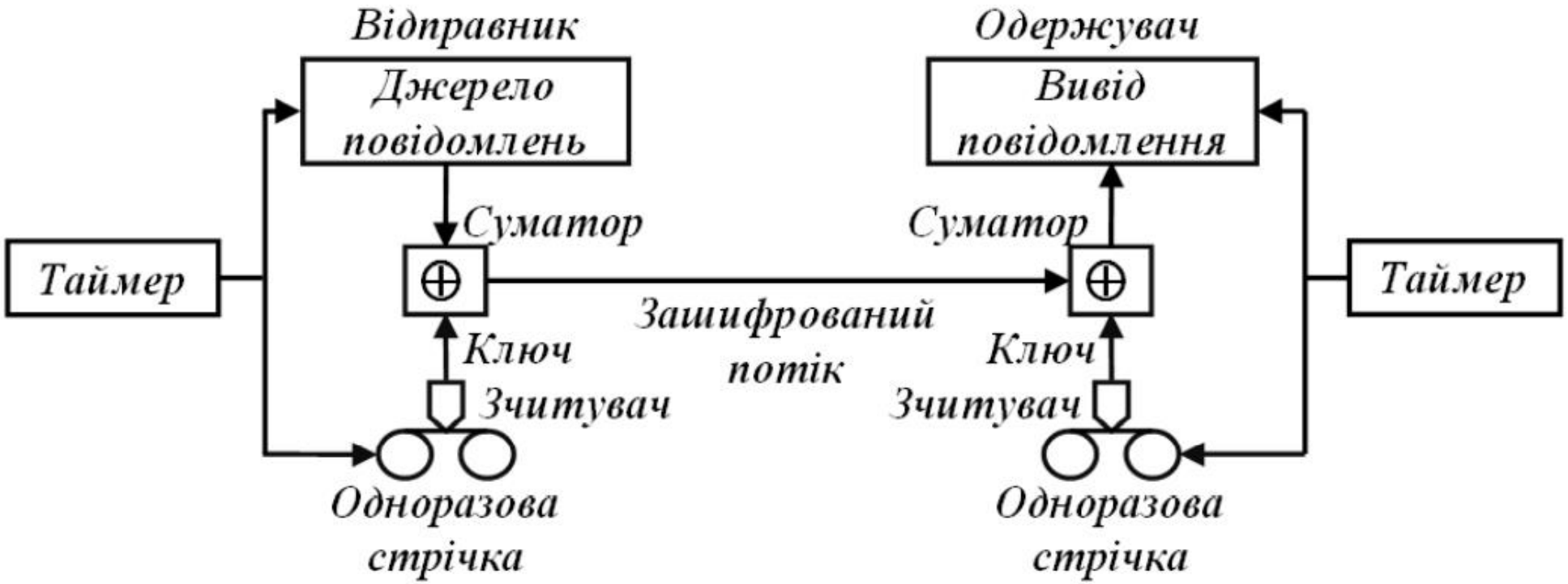
Шифр одноразового блокноту

One-time pad cipher - Абсолютно надійний шифр, який був винайдений у 1917 р. Г. Вернаном та Д. Моборном.



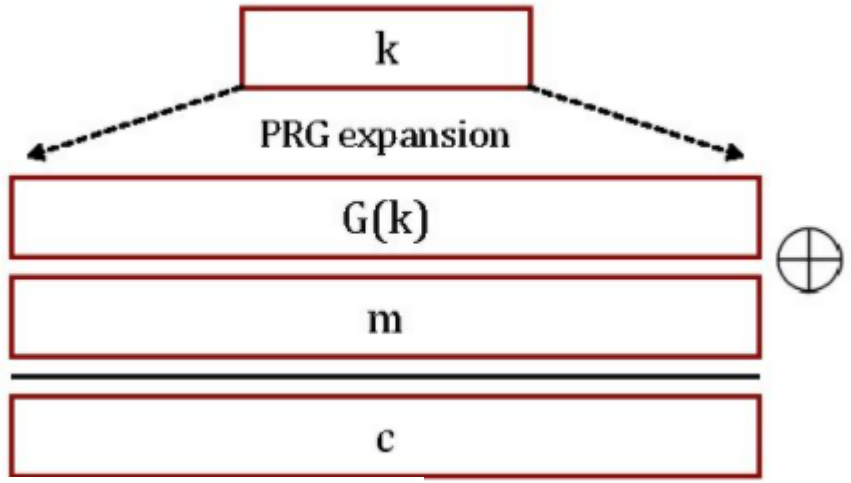

```
⊕ 00000100000001000100000010001
  00110111010110001001100011101 0
  ---------------------------------
  00110011010111001101100010101 1
```

Система Вернама

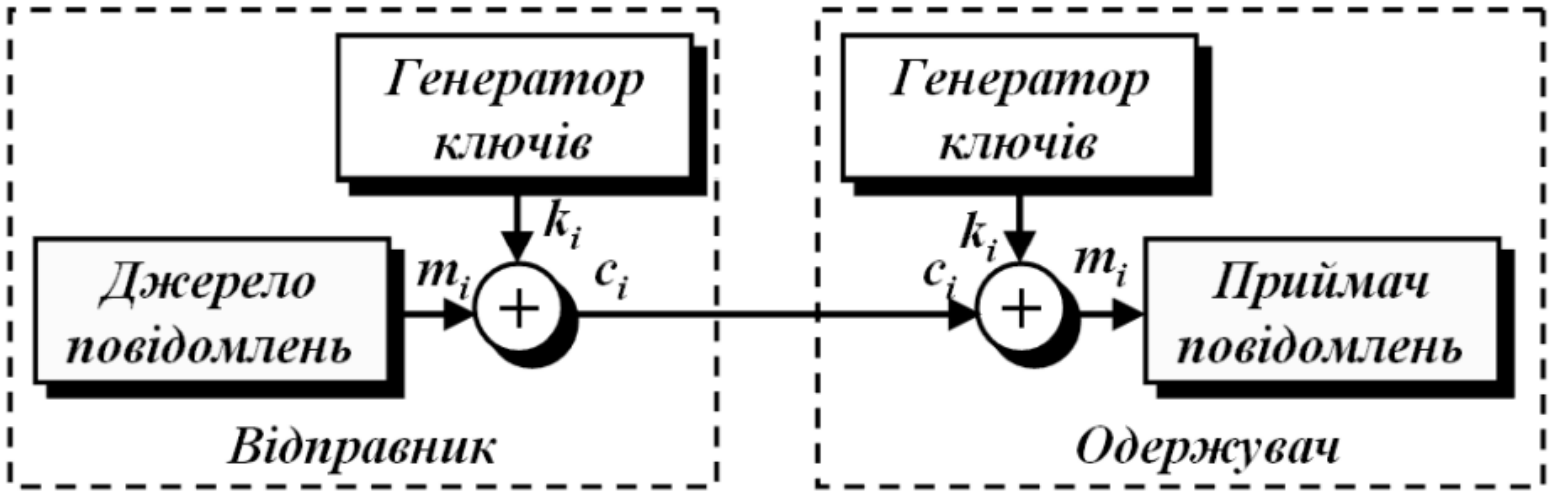


Потокові шифри

PRG можуть використовуватися як генератори ключів у потокових шифрах. Метою використання PRG є отримання нескінченного ключового слова, за використання відносно малої довжини самого ключа. PRG створює послідовність бітів, схожу на випадкову.



$G: \{0,1\}^s \rightarrow \{0,1\}^n, n \gg s;$
$C = E(k, m) := m \oplus G(k);\ D(k, c) := c \oplus G(k).$

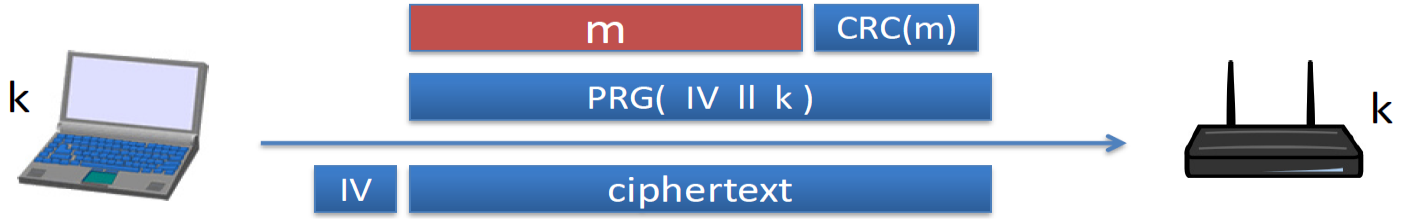


WEP 802.11b

Wired Equivalent Privacy (WEP) - найстаріший стандарт захисту бездротового трафіку, заснований на алгоритмі потокового шифрування RC4 (з використанням загального секретного ключа). Існують варіанти з довжиною ключа 64, 128 і 256 бітів.

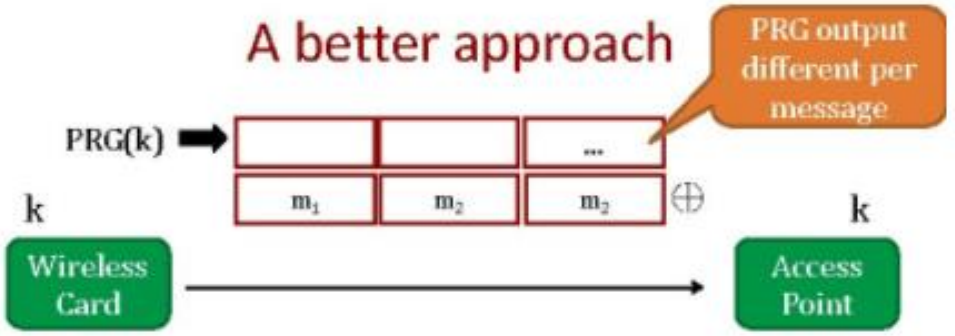
WPA (англ. Wi-Fi Protected Access) — один з протоколів безпеки для захисту бездротових мереж. Створений для заміни застарілого протоколу WEP. Заснований на TKIP (англ. Temporary Key Integrity Protocol — протокол тимчасової цілісності ключів), який ефективно бореться з проблемою, що лежить в основі вразливості WEP, — повторного використання ключів шифрування.

802.11b WEP:



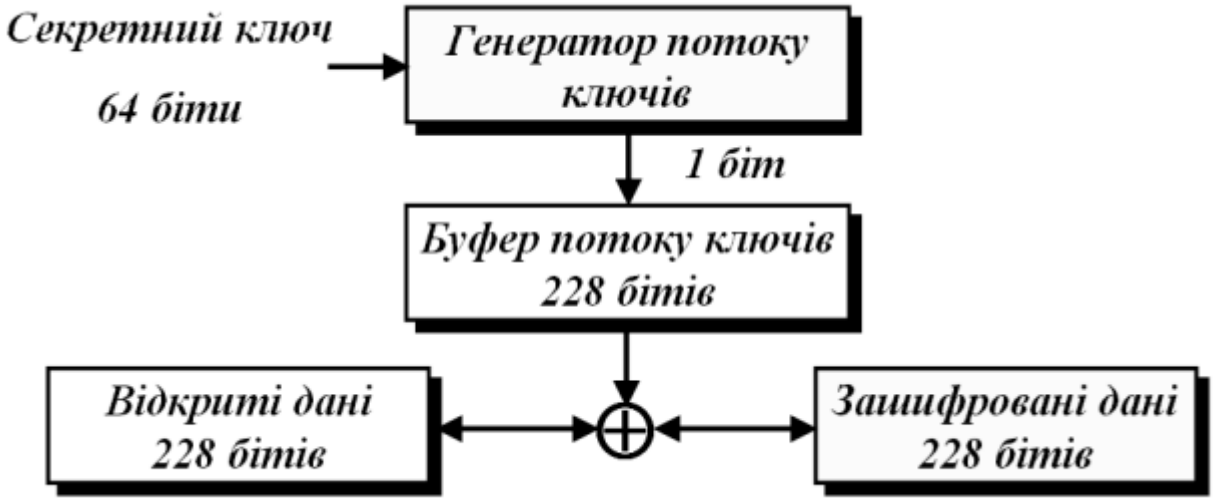
Length of IV: 24 bits

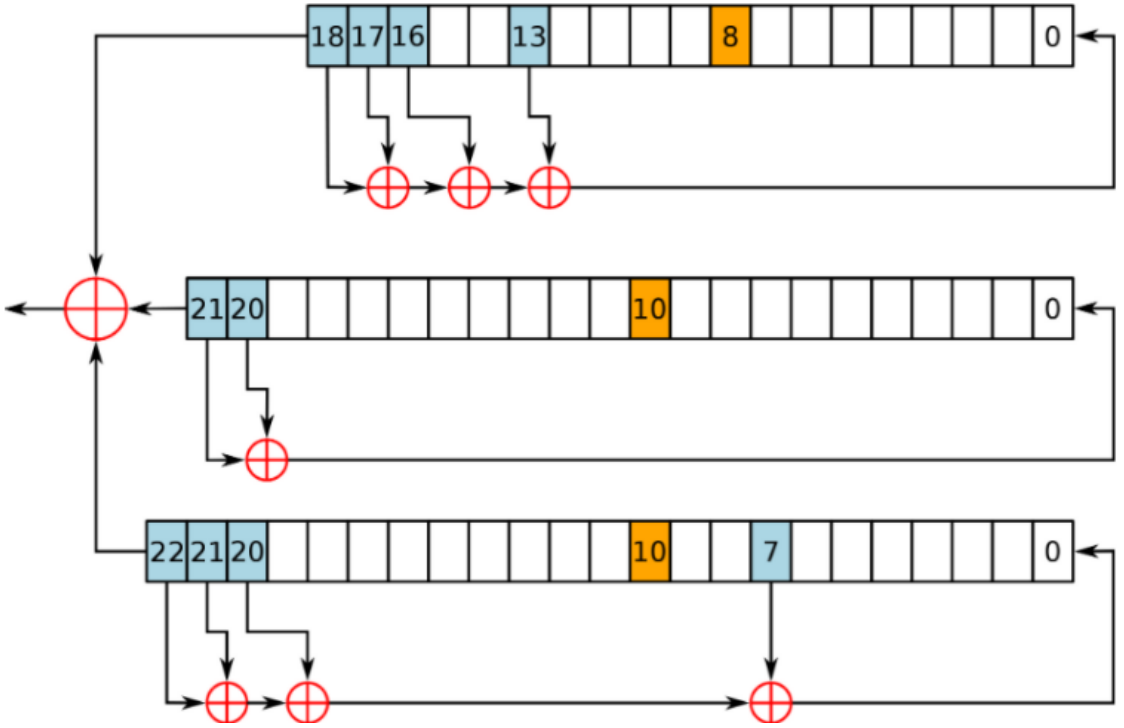
- Repeated IV after $2^{24} \approx 16M$ frames
- On some 802.11 cards: IV resets to 0 after power cycle



Потоковий шифр A5

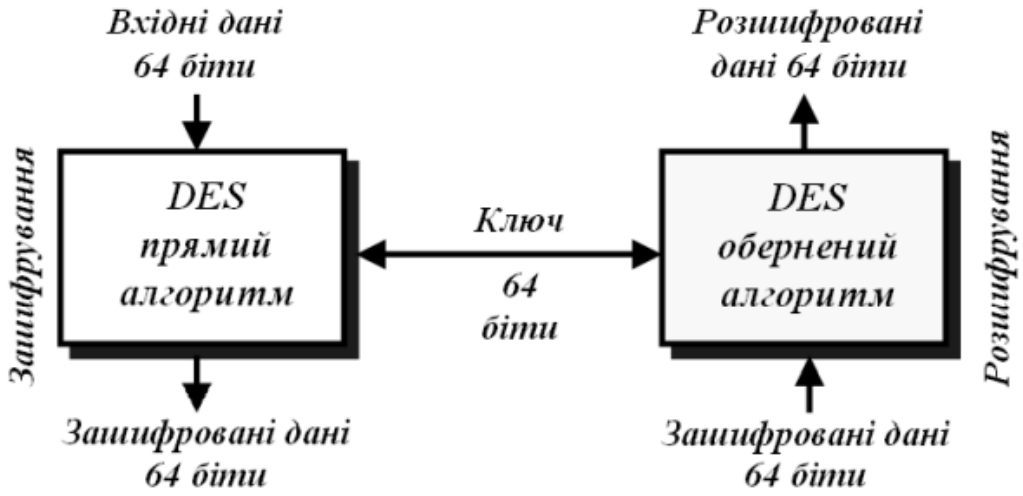
A5 — це потоковий алгоритм шифрування, що використовується для забезпечення конфіденційності даних, які передаються між телефоном і базовою станцією в європейській системі мобільного цифрового зв'язку GSM (Group Special Mobile). Цей шифр забезпечував достатній рівень захищеності потоку, що забезпечувало конфіденційність розмови. Спочатку експорт стандарту з Європи не передбачався, але незабаром у цьому з'явилася необхідність. Саме тому, A5 перейменували в A5/1 і стали поширювати в Європі та США. Для решти країн алгоритм модифікували, значно знизивши криптографічну стійкість шифру. A5/2 був спеціально розроблений як експортний варіант для країн, що не входили до Євросоюзу.

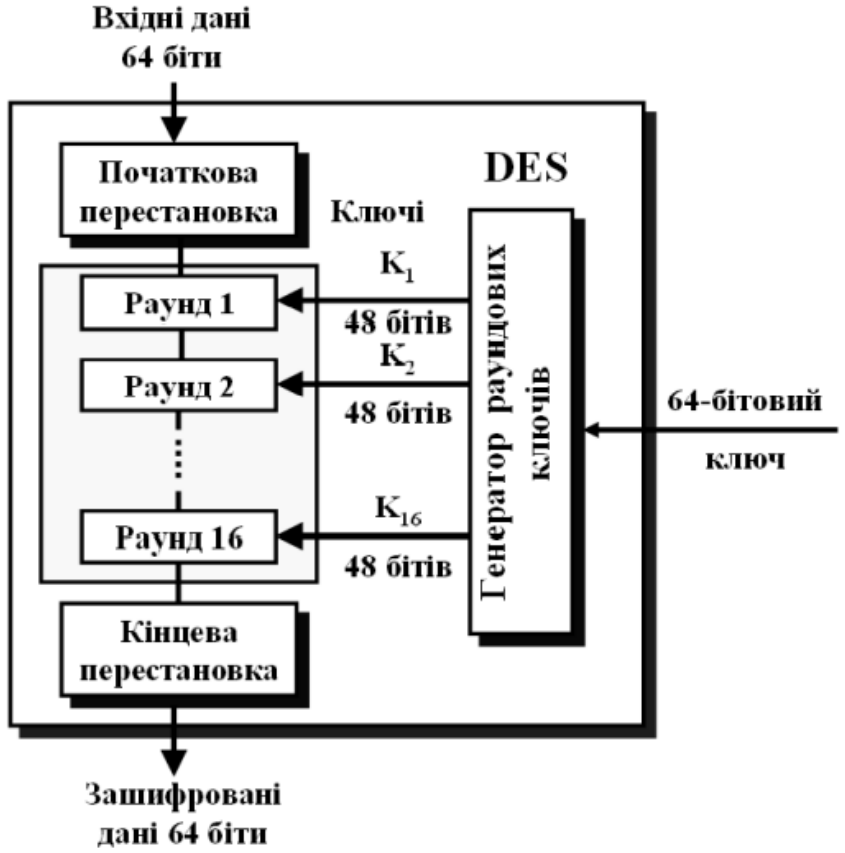




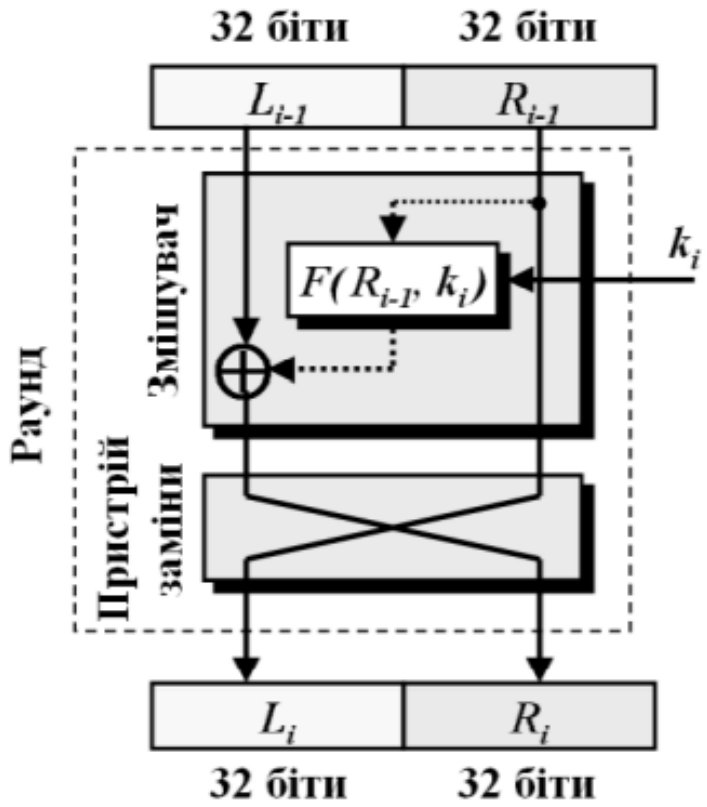
Стандарт шифрування даних DES

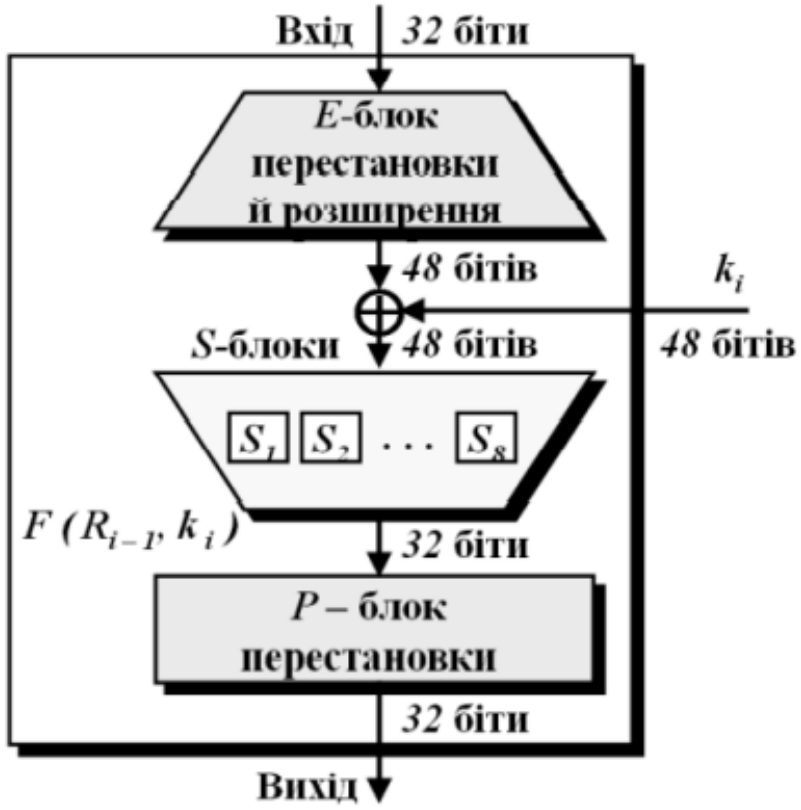
Запропонована IBM модифікація проекту, названа “Люцифер” (Lucifer), була прийнята як DES, стандарт шифрування прийнятий урядом США із 1976 до кінця 1990-х, з часом набув міжнародного застосування. У 1999 ключ DES було публічно дешифровано за 22 години 15 хвилин.





Процес шифрування даних DES

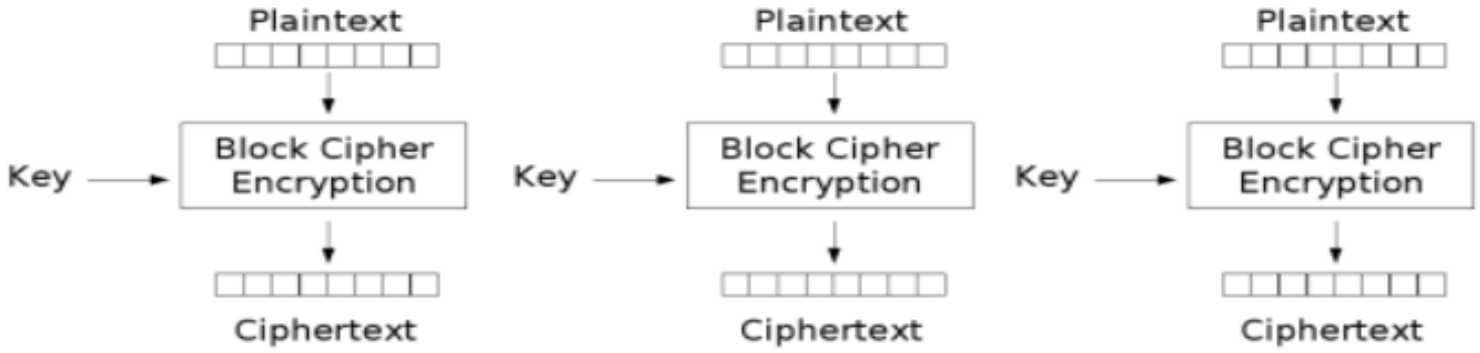




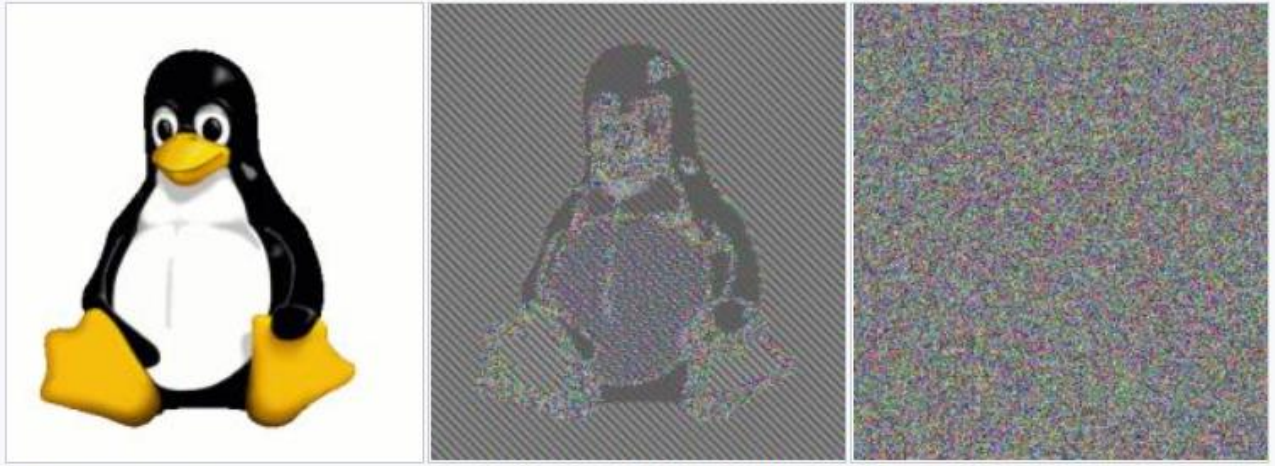
$$L_i = R_i;$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, k_i),\ i = 1,2,..,16,$$

Режим електронної кодової книги (ECB)



Electronic Codebook (ECB) mode encryption

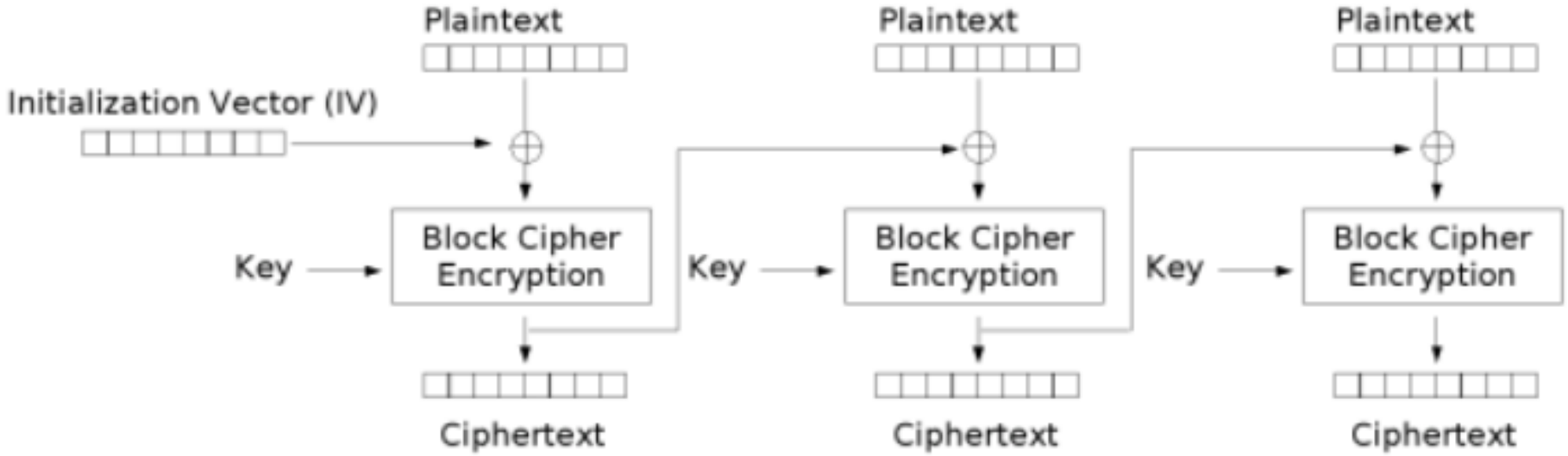


Первісне зображення | зашифроване в режимі ECB | Псевдовипадковий вислід режимів відмінних від ECB

Режим зчеплення шифроблоків (CBC)

IBM винайшла режим зчеплення шифроблоків (англ. cipher-block chaining, CBC) у 1976.[5] Кожен шифроблок, залежить від усіх блоків оброблених до нього. Для отримання унікальних повідомлень потрібно використовувати ініціалізаційний вектор у першому блоці.

$$C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV,$$

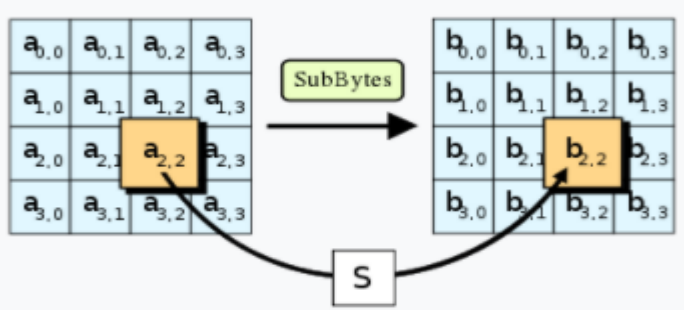


Cipher Block Chaining (CBC) mode encryption

Стандарт шифрування даних AES

Advanced Encryption Standard (AES) - симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128/192/256 біт), прийнятий як американський стандарт шифрування урядом США (2002 р).

Алгоритм блокового шифрування

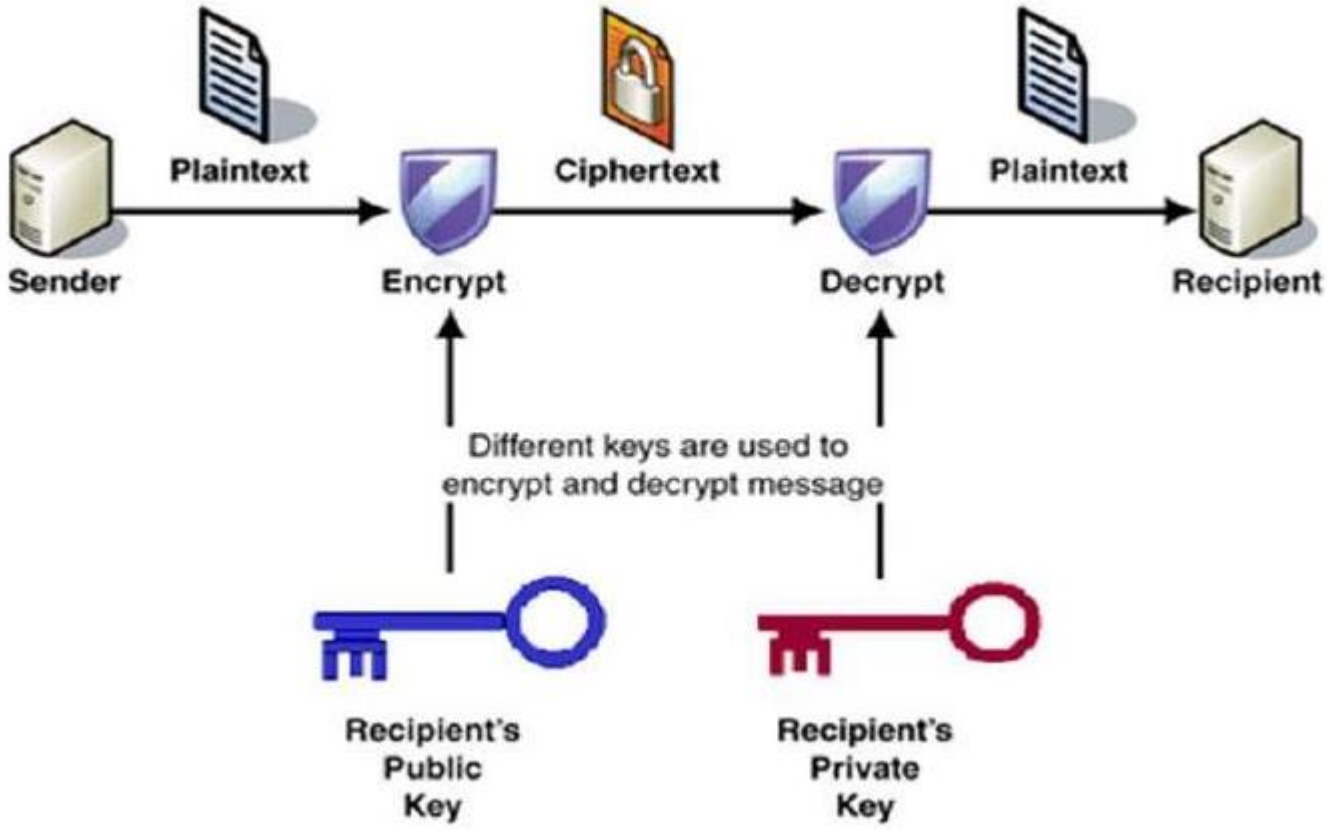


Назва:	AES, Rijndael-AES, Rijndael
Розробник:	В.Реймен, Д.Даймон
Створений:	1998 р.
Опублікований:	2001 р.
Розмір ключа:	128/192/256 біт
Розмір блоку:	128 біт
Число раундів:	10/12/14
Тип:	SP-мережа

Асиметричні криптосистеми

Криптосистеми з відкритим ключем

1976 рік відкрив сучасний етап у криптографії. Американські математики Вайтфілда Діффі та Мартіна Гелмана, а також Ральфа Меркле запропонували ідеологію відкритого ключа.



Криптосистема RSA

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 Ейлера 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. Для e за алгоритмом Евкліда знаходить елемент d, обернений до e в $Z^*_{\phi(n)}$, тобто такий, що $d < \phi(n)$ і $ed \equiv 1 (\mathrm{mod}\ \phi(n))$

Відкритий ключ: *e, n*;

Таємний ключ: *d*;

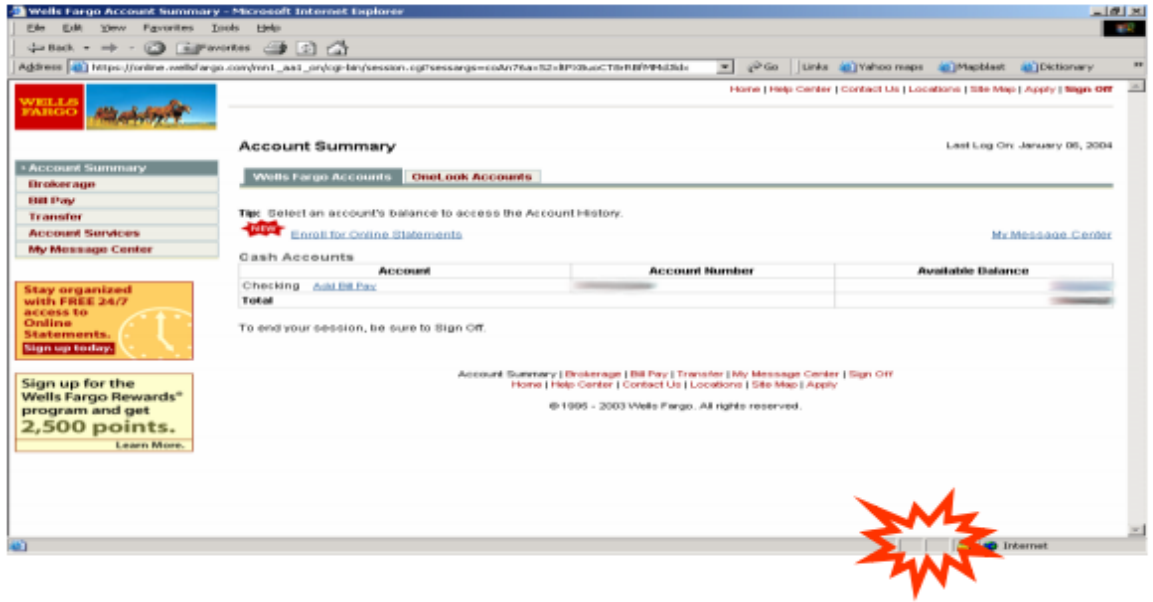
Шифрування: $E(M) = M^e mod\ n$;

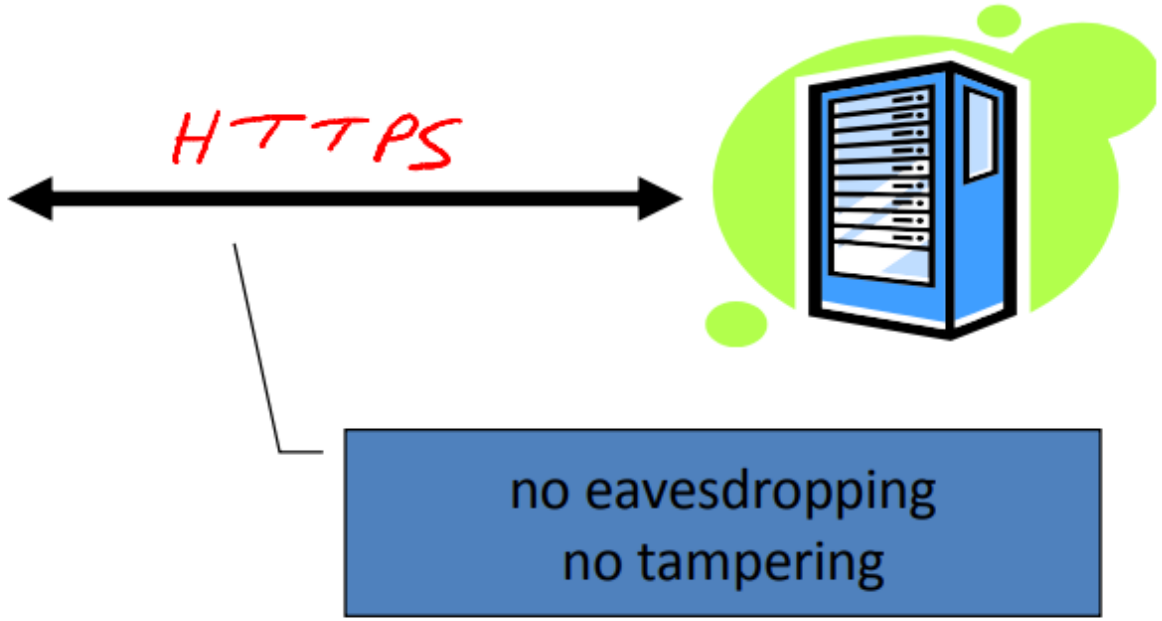
Дешифрування: $D(C) = C^d mod\ n$.

Застосування криптографічних систем

Шифрування інформаційного потоку

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





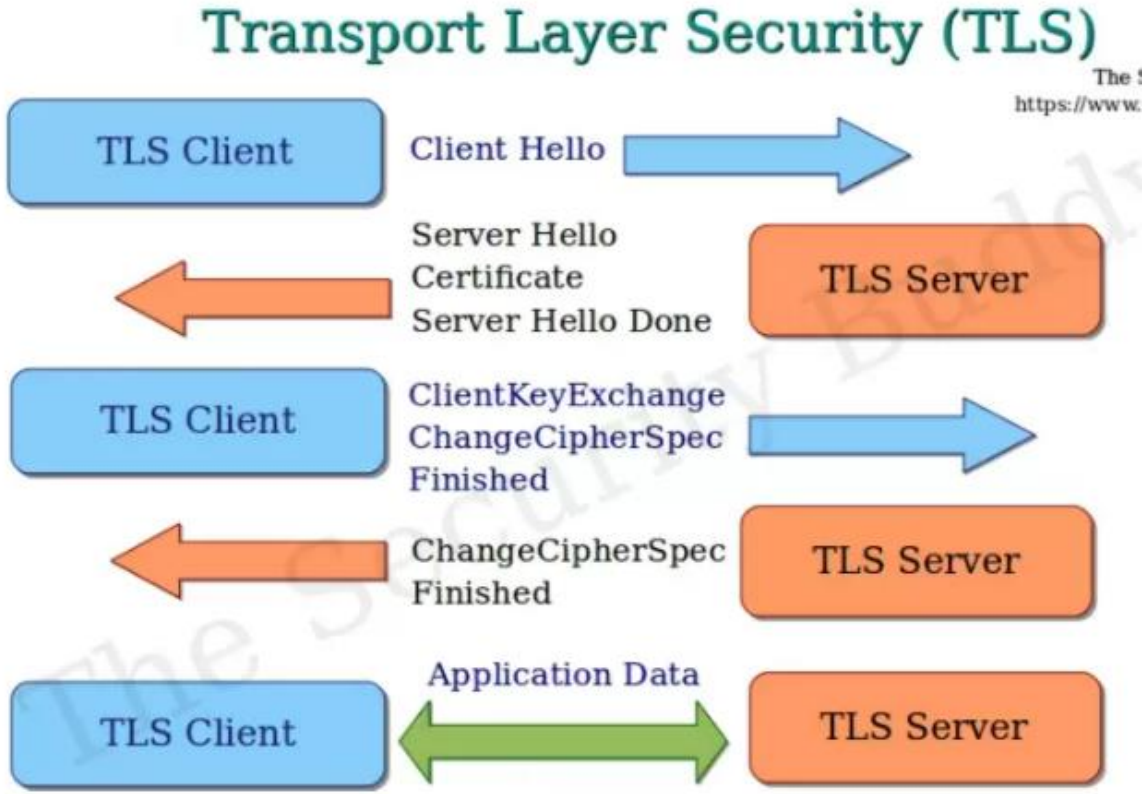
Криптографічний протокол SSL/ TLS

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

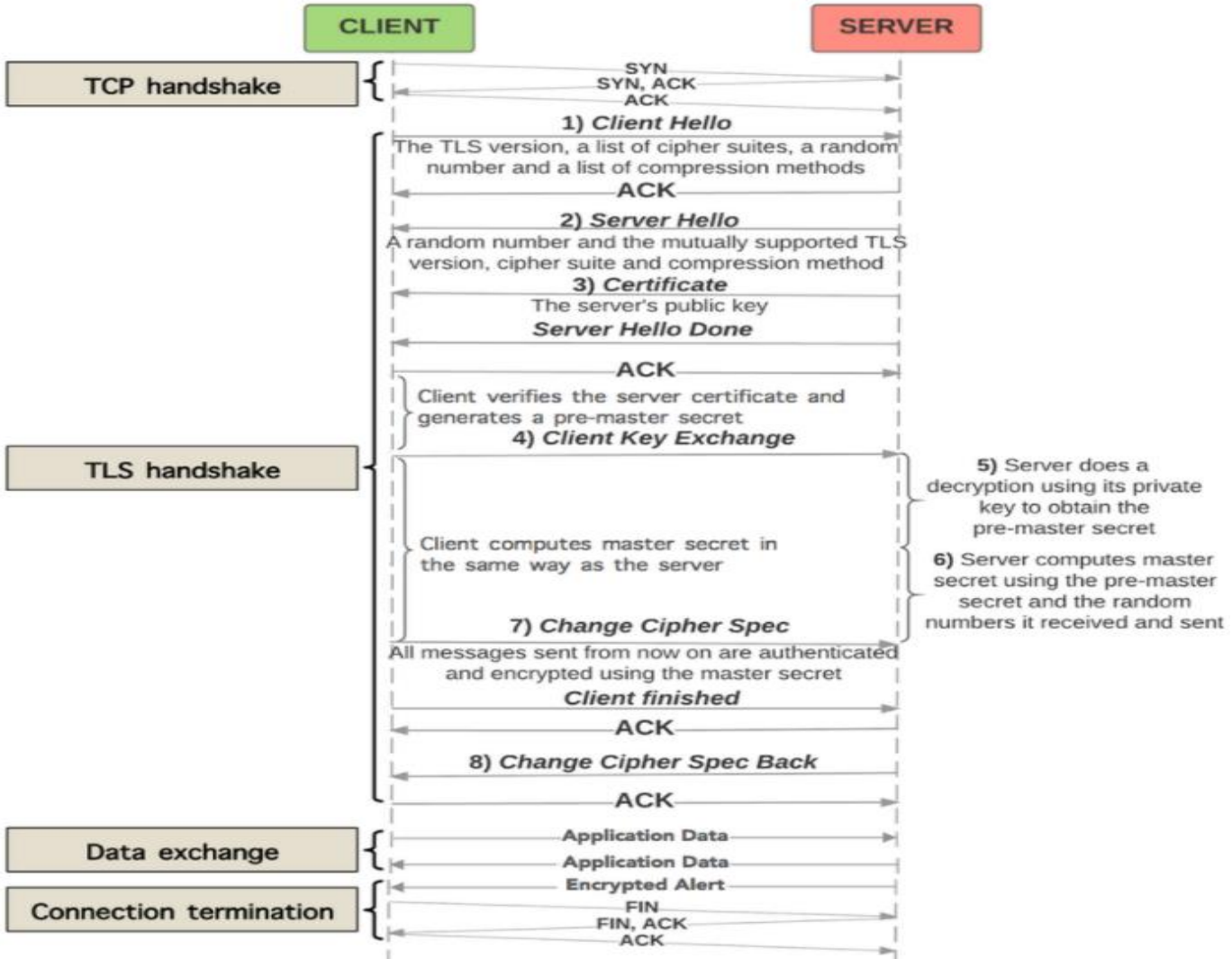
Криптографічним протоколом називається такий, в основі якого лежить криптографічний алгоритм.

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



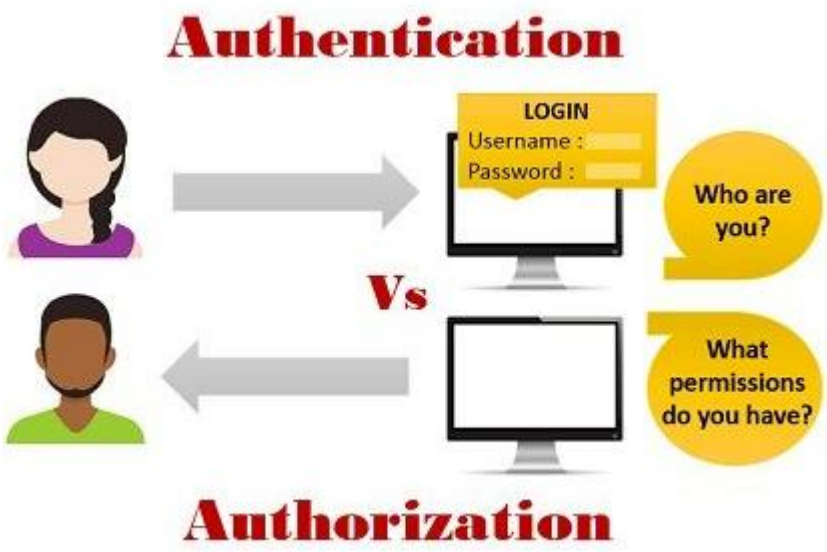
Протокол обміну Diffie–Hellman

- 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:

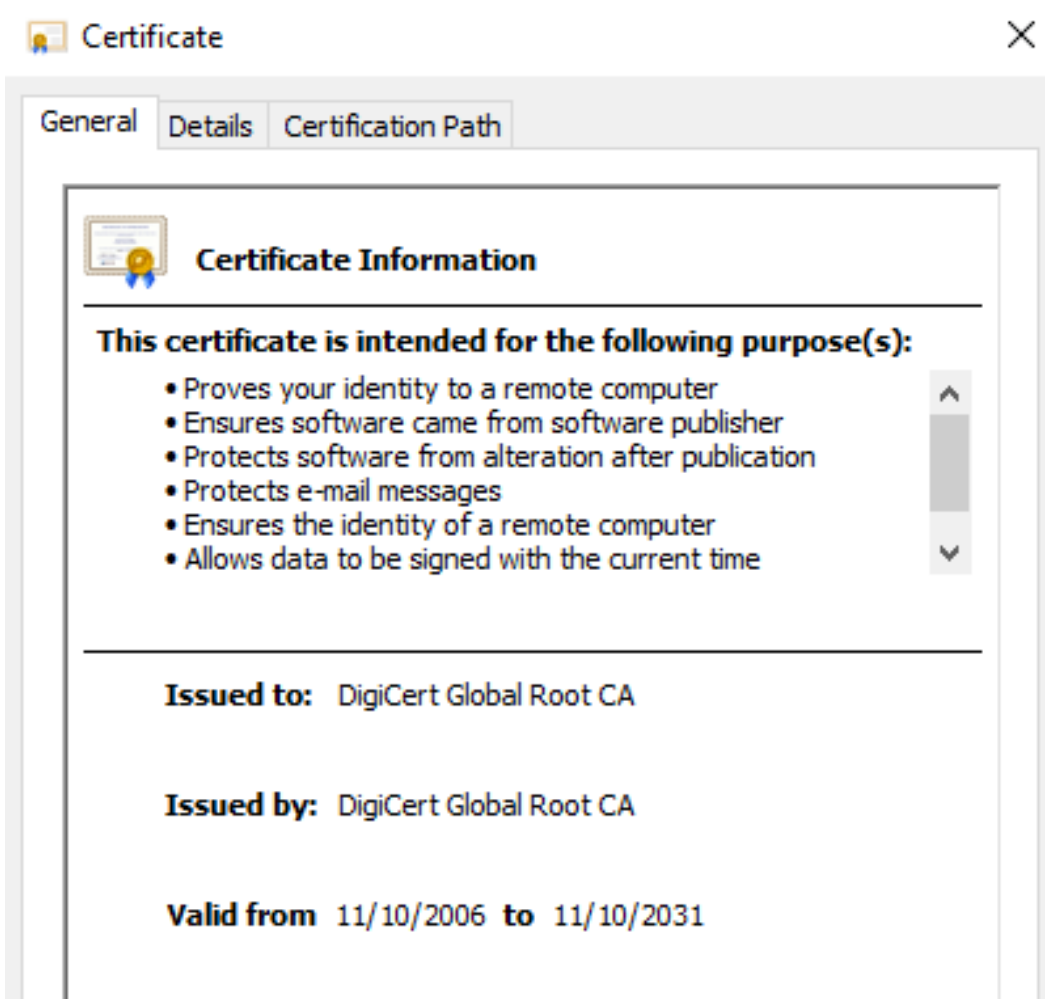
$$(g^b)^a mod \, p = (g^a)^b mod \, p = g^{ab} mod \, p.$$

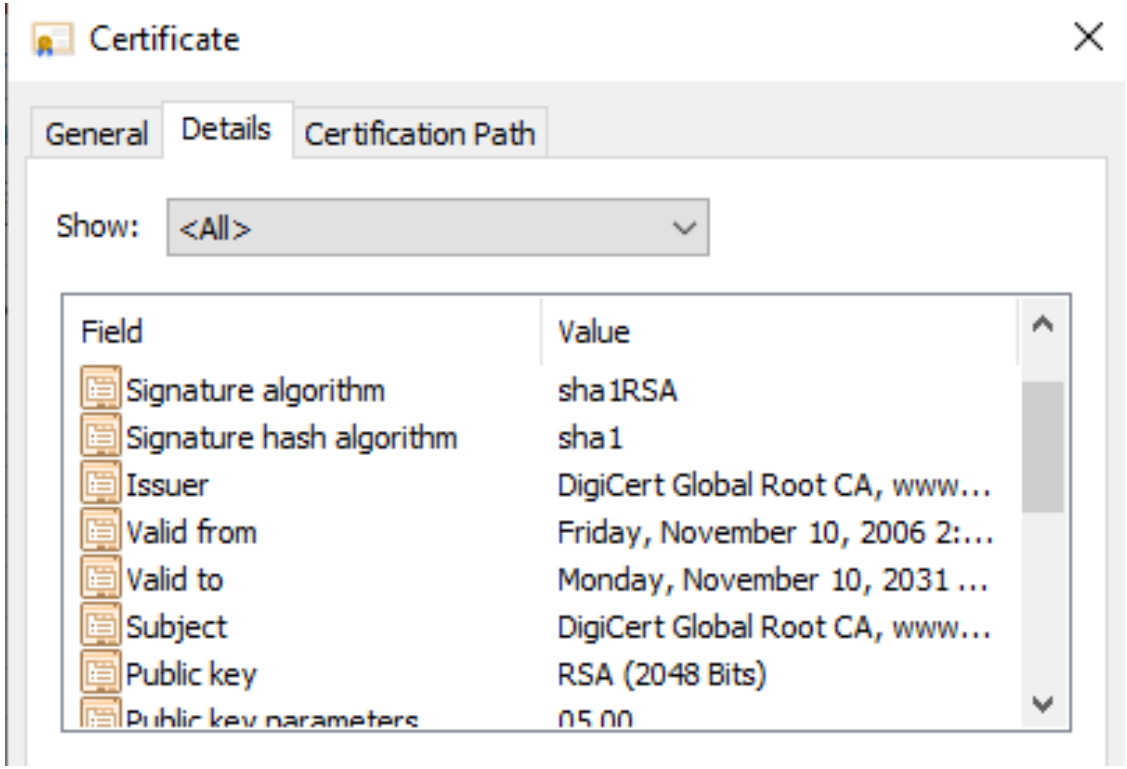
Схематична ілюстрація протоколу на прикладі змішування фарб

Автентифікація та авторизація



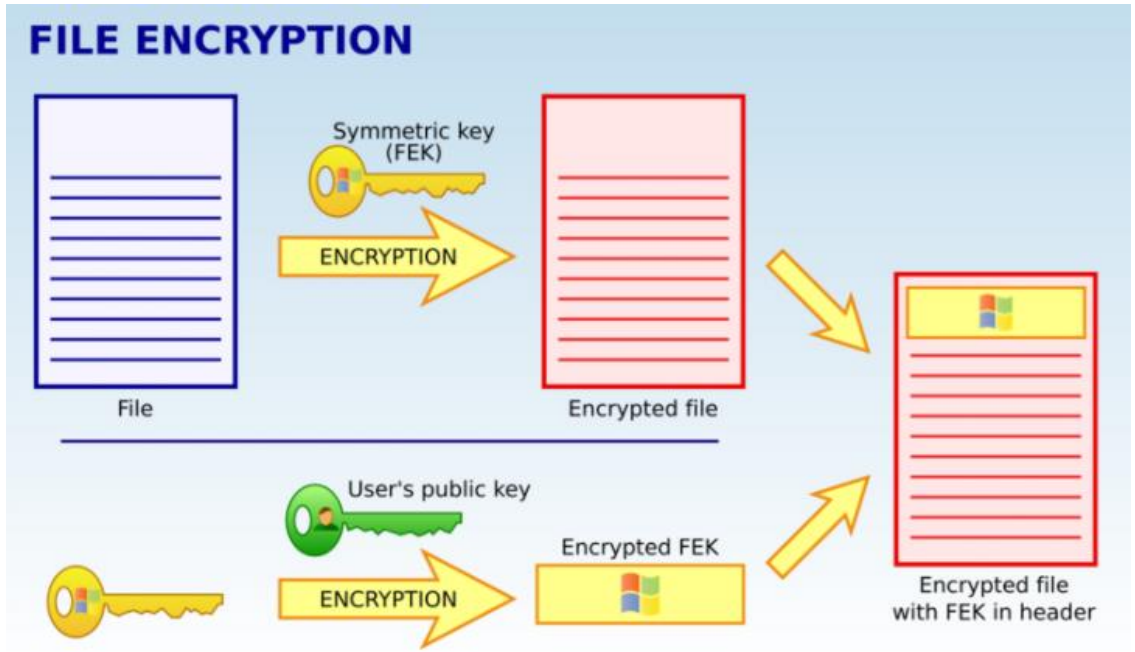
Цифровий сертифікат

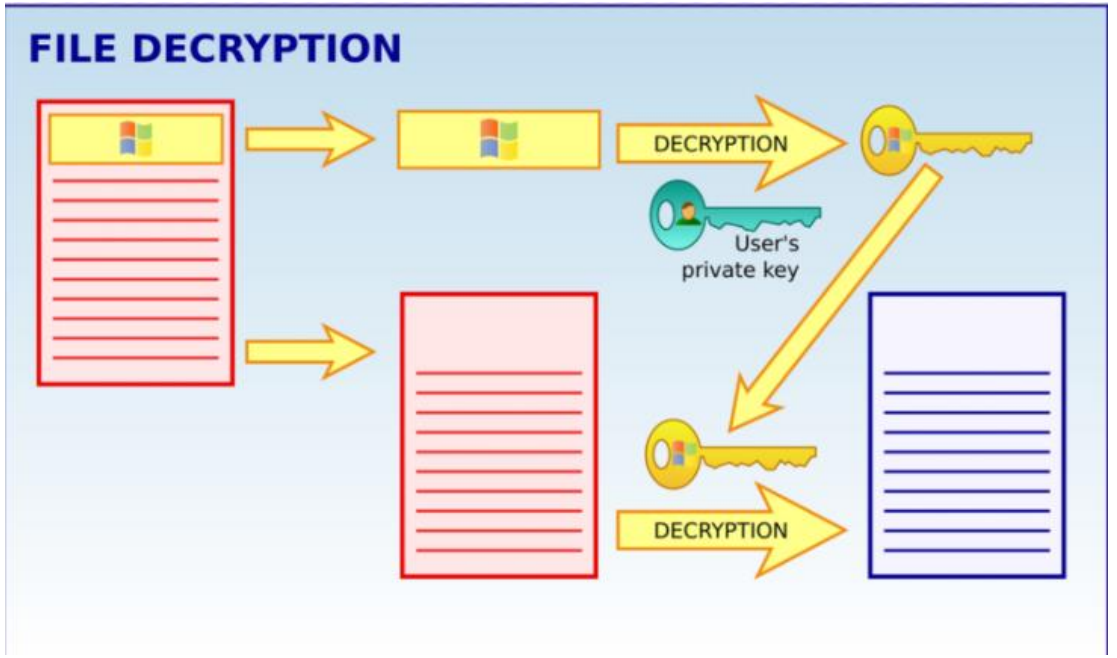




Захист даних на диску

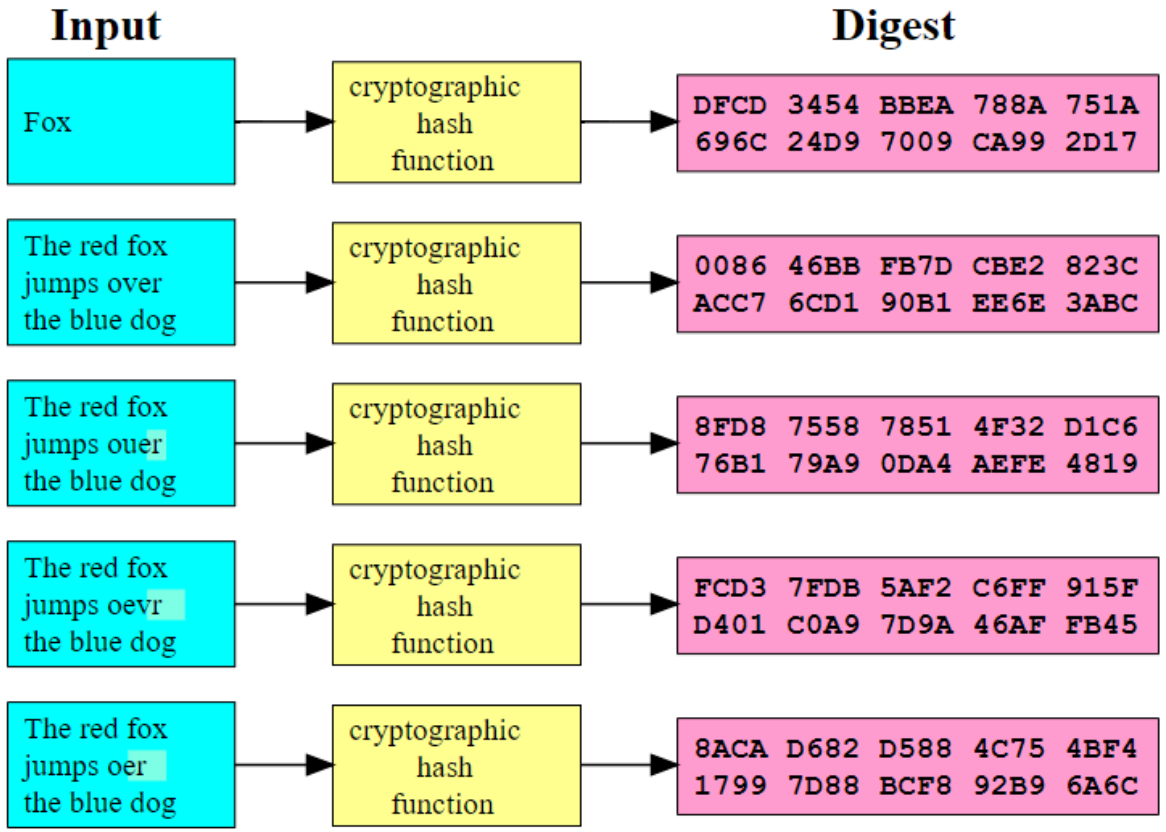
- **Encrypting File System (EFS)** — система шифрування даних, що реалізує шифрування на рівні файлів в операційних системах (Windows).
- **TrueCrypt, VeraCrypt** — програмне забезпечення для шифрування дисків та файлі. Використовує симетричні алгоритми шифрування AES, Twofish, Seprent.





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)).



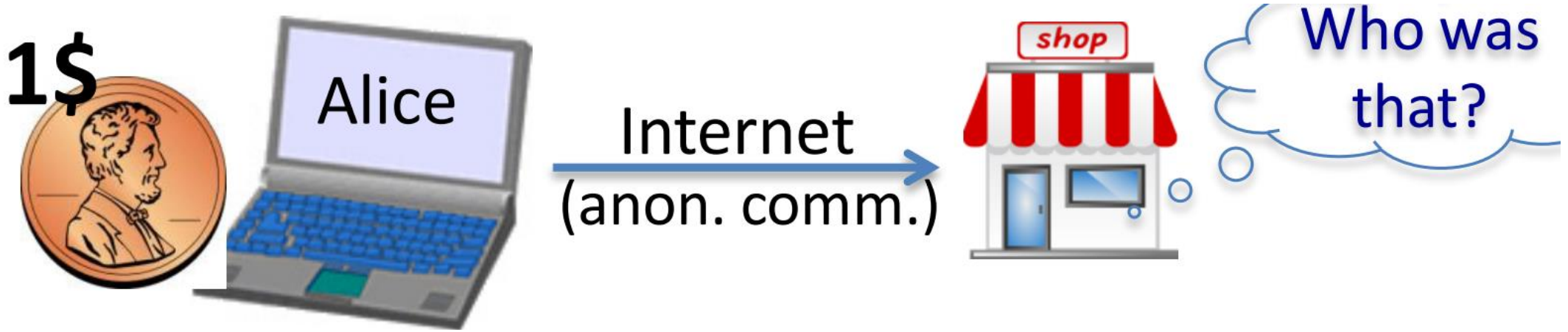
Електронний цифровий підпис

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?



OpenSSL

OpenSSL - відкритий програмний продукт, розроблений як універсальна бібліотека для криптографії, що використовує протоколи SSL та TLS. Використовується, зокрема, в бібліотеці cUrl для реалізації роботи за протоколом https.

Examples of commands:

```
$ openssl list -cipher-algorithms
$ openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out private-key.pem
$ openssl pkey -in private-key.pem -text
$ openssl pkey -in private-key.pem -pubout -out public-key.pem
$ openssl pkey -in public-key.pem -pubin –text
$ openssl list -digest-commands
$ openssl md5 test.txt
$ openssl enc -aes-256-cbc -e -iter 1000 -salt -in test.txt -out test.enc
$ openssl enc -aes-256-cbc -d -iter 1000 -in test.enc -out test.dec
```

Онлайн курси

- https://www.coursera.org/learn/crypto
- https://www.coursera.org/learn/crypto2
- **https://ua.udemy.com/course/learn-cryptography-basics-in-python/learn/lecture/10371350#overview**
- https://www.udacity.com/course/applied-cryptography--cs387
- https://www.udemy.com/course/learn-modern-security-and-cryptography-by-coding-in-python/
- https://www.udemy.com/course/conversation-on-cryptography-a-total-course-w-mike-meyers/
- https://www.udemy.com/course/cryptography-learn-public-key-infrastructure-or-pki-from-scratch/
- https://www.udemy.com/course/encryption-and-cryptography-for-professionals/

Рекомендована літератера

1. *Вербіцький О.В.* Вступ до криптології. Львів, 1998;
2. *Корченко О.Г., Сіденко В.П. , Дрейс Ю.О.* Прикладна криптологія. Житомир, 2014;
3. *Paar C, · Pelzl J.* Understanding Cryptography. A Textbook for Students and Practitioners, 2010;
4. *Schneier B.* Applied cryptography, second edition, protocols, algorithms, and source code in C, 1996;
5. *Nigel P. Smart.* Cryptography Made Simple, 2016;
6. *Wong D.* Real-World Cryptography, Version 12, 2021 Manning Publications;
7. *Stallings W.* Cryptography and network security. Principles and practice. Seventh edition. Global edition, 2017.

Дякую за увагу!