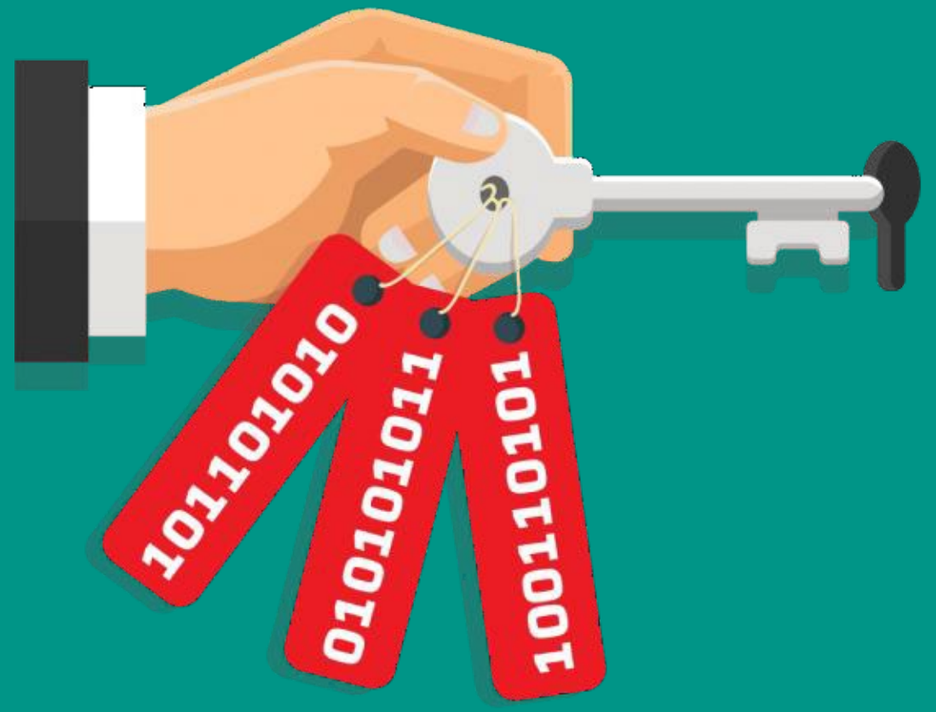
ЛЕКЦІЯ 3

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Криптографічна стійкість шифрів



План

1. Поняття криптографічної стійкості

2. Абсолютно стійкий шифр

3. Типи атак на криптосистеми

1. Поняття криптографічної стійкості

Основні принципи Керкгоффа

1. Система має бути безпечною, навіть якщо всі її деталі, крім ключа, відомі публіці.
2. Стійкість системи повинна залежати виключно від секретності ключа.
3. Ключ має легко передаватися та, за потреби, бути зміненим.
4. Шифротекст повинен бути стійким до відгадування ключа.
5. Шифр має бути простим у використанні та реалізації.
6. Система повинна бути придатною для комунікацій.

1. Поняття криптографічної стійкості

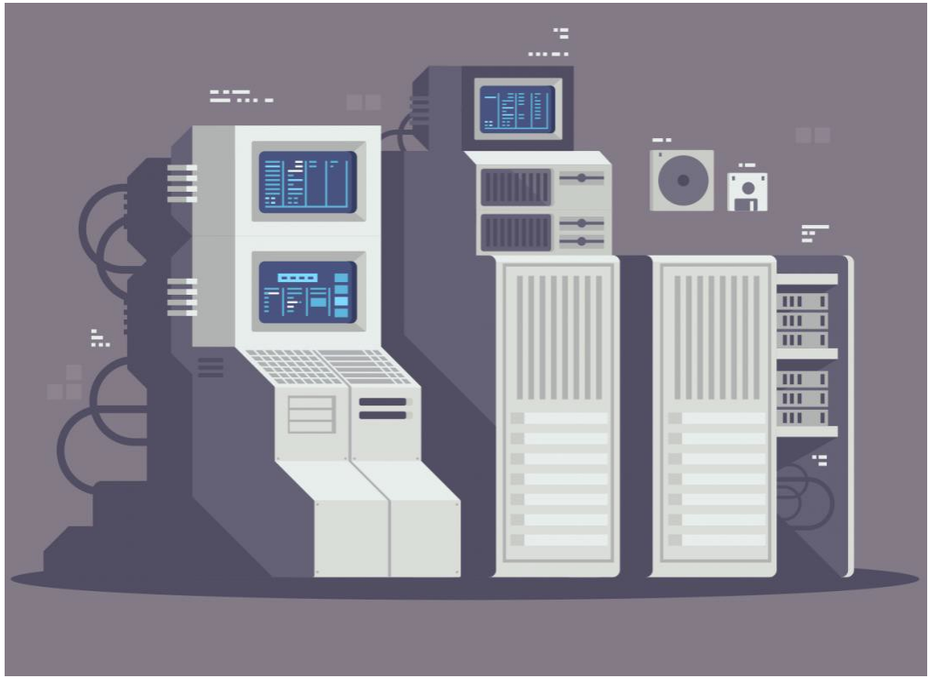
Роль ключів у забезпеченні криптографічної стійкості

1. Довжина ключа визначає рівень стійкості до атаки методом грубої сили: чим більший ключ, тим безпечніша система.
2. Надійна генерація з високою ентропією забезпечує криптографічну стійкість і непередбачуваність ключів.
3. Вразливості через слабку генерацію ключів можуть поставити під загрозу всю систему шифрування.

1. Поняття криптографічної стійкості

Види стійкості шифрів (по Шеннону)

Теоретична (абсолютна) стійкість – стійкість криптосистеми за наявності у криптоаналітика необмеженого часу, необмежених обчислювальних ресурсів, найкращих методів криптоаналізу



Оцінка базується на теорії інформації та теорії ймовірностей

1. Поняття криптографічної стійкості

Види стійкості шифрів (по Шеннону)

Практична (обчислювальна) стійкість – стійкість криптосистеми на поточний момент часу з урахуванням того, що криптоаналітик володіє сучасними методами криптоаналізу, проте час та обчислювальні ресурси обмежені

Оцінка базується на теорії складності

1. Поняття криптографічної стійкості

Показники стійкості криптосистеми

1. Час, необхідний для реалізації атаки на доступних/перспективних обчислювальних засобах.

2. Обсяг пам'яті, необхідний для виконання криптографічного аналізу.

3. Мінімально необхідна для успішної реалізації атаки кількість пар «відкритий текст – шифротекст».

1. Поняття криптографічної стійкості

Властивості притаманні стійким шифрам

Розсіювання (перестановка)

поширення впливу одного знаку відкритого тексту, а також одного знаку ключа на значну кількість знаків зашифрованого повідомлення

Перемішування (підстановка)

маскування взаємозв'язку статистичних властивостей відкритого тексту та шифротексту

1. Поняття криптографічної стійкості

Умови стійкості шифрів

- Достатня довжина ключа
- Відсутність слабких ключів
- Висока ентропія шифротексту
- Чутливість до малих змін вхідних даних (лавинний ефект)
- Захищеність від диференціальних і лінійних криптоаналітичних атак
- Незалежність ключа і відкритого тексту
- Стійкість до атак по сторонніх каналах
- Захищеність від квантових атак
- Використання перевірених алгоритмів та стандартів
- Захищеність від обхідних атак та модифікацій

2. Абсолютно стійкий шифр

Творці – Гільберт Вернам зі співробітниками телеграфної компанії AT&T, а також офіцер армії США Джозеф Моборн (1917 рік)

Шифр Вернама є єдиною системою шифрування, для якої доведена абсолютна криптографічна стійкість (Клод Шеннон, 1949 рік)

Гільберт Вернам

Джозеф Моборн

2. Абсолютно стійкий шифр

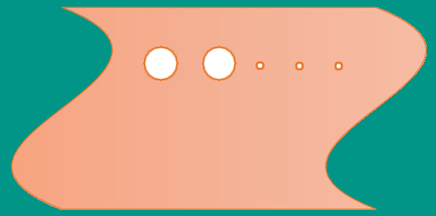
Ідея автоматичного шифрування телеграфних повідомлень

Відкритий текст представлявся у вигляді п'ятизначних імпульсних комбінацій на перфострічці

Ключ: перфострічка з випадковими знаками – «гама»

Наприклад, літера «А» мала вигляд:

+ + - - -



«+» – отвір

«-» – його відсутність

2. Абсолютно стійкий шифр

Шифрування:

імпульси «гами» електромеханічно складалися з імпульсами знаків відкритого тексту. Отримана сума представляла собою шифротекст

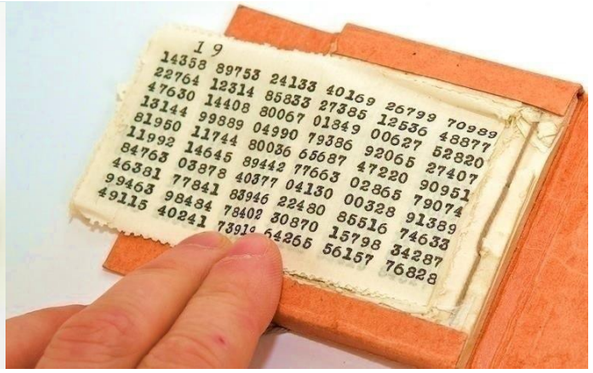
Дешифрування:

імпульси, отримані по каналу зв'язку, електромеханічно складалися з імпульсами тієї самої «гами», в результаті чого відновлювалися вихідні імпульси повідомлення

2. Абсолютно стійкий шифр

Класичний одноразовий блокнот

Ключ: одноразовий блокнот – послідовність випадкових символів, написаних на аркушах паперу



Ключ повинен володіти трьома критично важливими властивостями:

1) бути дійсно випадковим;

2) за розміром збігатися з заданим відкритим текстом (ключ ні в якому разі не зациклюється)

3) застосовуватися тільки один раз!

2. Абсолютно стійкий шифр

Шифрування:

кожен символ ключа використовується для шифрування одного символу повідомлення

Дешифрування:

одержувач, використовуючи точно такий самий блокнот, дешифрує кожний символ шифротексту

2. Абсолютно стійкий шифр

Приклад 3.1:
Ключ: XVHEUWNOPGDZ
Повідомлення: THIS IS SECRET
Шифрування:

Відкритий текст	19 07 08 18 08 18 18 04 02 17 04 19
Ключ	23 21 07 04 20 22 13 14 15 06 03 25
Результат додавання	42 28 15 22 28 40 31 18 17 23 07 44
За модулем 26	16 02 15 22 02 14 05 18 17 23 07 18
Шифротекст	QCPWCOFSRXHS

2. Абсолютно стійкий шифр

Приклад 3.2:
Ключ: XVHEUWNOPGDZ
Шифротекст: QCPWCOFSRXHS
Дешифрування:

Шифротекст	16 02 15 22 02 14 05 18 17 23 07 18
Ключ	23 21 07 04 20 22 13 14 15 06 03 25
Результат віднімання	-7 -19 08 18 -18 -8 -8 04 02 17 04 -7
За модулем 26	19 07 08 18 08 18 18 04 02 17 04 19
Відкритий текст	THIS IS SECRET

2. Абсолютно стійкий шифр

Для шифрування бінарних даних (потоку бітів)

Ключ: послідовність випадкових бітів

⊕	0	1
0	0	1
1	1	0

Виконується додавання бітів за модулем 2 (операція XOR, eXclusive OR – виключне або)

2. Абсолютно стійкий шифр

Приклад 3.3:
Ключ: 00001011 00010010 00001111
Повідомлення: SUN
Шифрування:

Відкритий текст	01010011 01010101 01001110
Ключ	00001011 00010010 00001111
Результат додавання за модулем 2	01011000 01000111 01000001
Шифротекст	XGA

2. Абсолютно стійкий шифр

Чому ж не використовують абсолютно стійкий шифр?

Навіщо придумали інші шифри, якщо вони не ідеальні?

Недоліки:

- ✓ проблема генерації та зберігання ключа;
- ✓ проблема передавання ключа для дешифування.

3. Типи атак на криптосистеми

Атака грубої сили (brute force attack)

Перебір усіх можливих ключів для знаходження правильного, який розшифрує зашифрований текст.

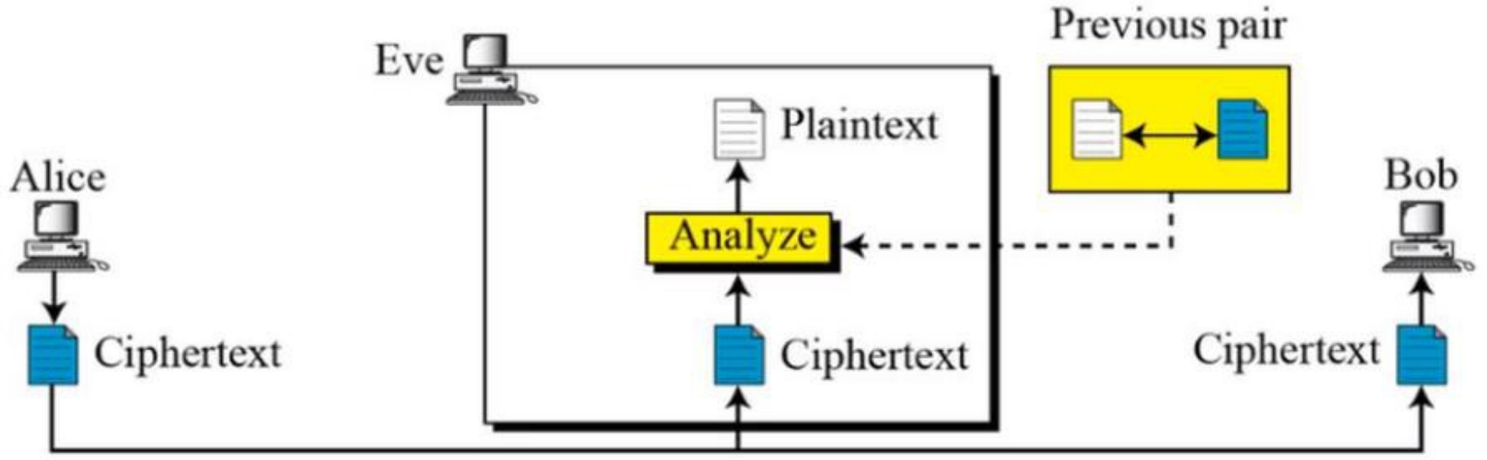
Key	Key	Worst case time at speed:		
length	space	10^9/sec	10^{12}/sec	10^{15}/sec
32	2^{32}	4 sec	4 ms	4 us
56	2^{56}	833 days	20 hrs	72 sec
64	2^{64}	584 yrs	213 days	5 hrs
80	2^{80}	10^7 yrs	10^4 yrs	38 yrs

Key	Key	Worst case time at speed:		
length	space	10^9/sec	10^{12}/sec	10^{15}/sec
100	2^{100}	10^{13} yrs	10^{10} yrs	10^7 yrs
128	2^{128}	10^{22} yrs	10^{19} yrs	10^{16} yrs
192	2^{192}	10^{41} yrs	10^{38} yrs	10^{35} yrs
256	2^{256}	10^{60} yrs	10^{57} yrs	10^{54} yrs

3. Типи атак на криптосистеми

Атака на основі відкритого тексту (known-plaintext attack)

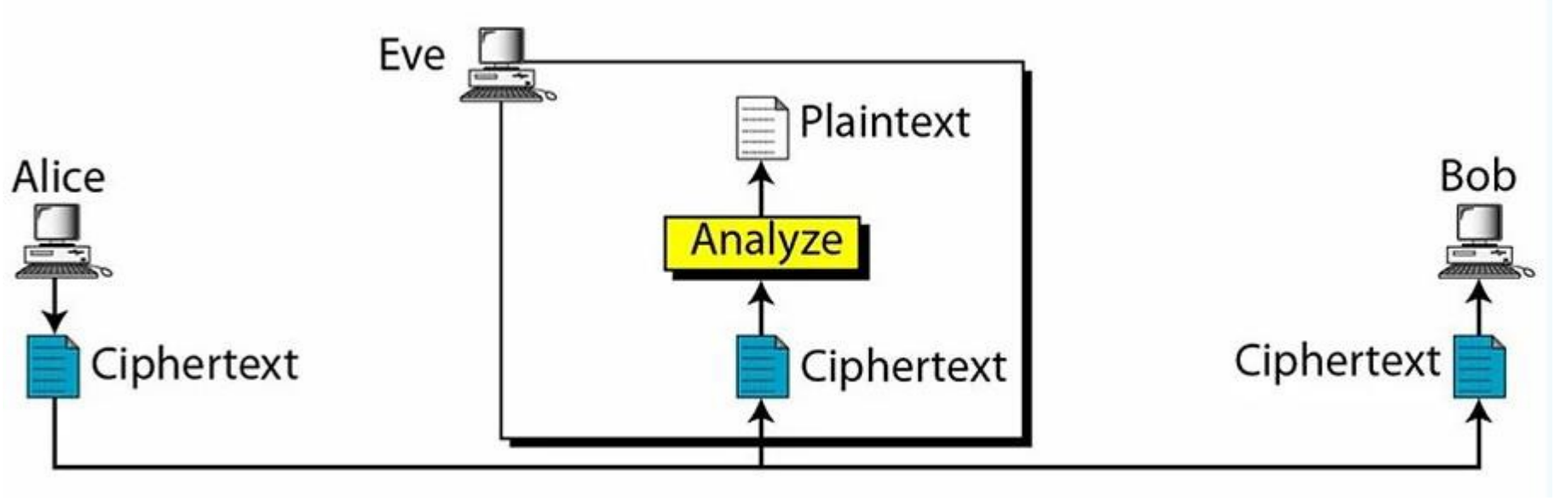
Криптоаналітик має доступ, принаймні, до обмеженої кількості пар відкритого тексту та відповідного шифрованого тексту.



3. Типи атак на криптосистеми

Атака на основі шифротексту (ciphertext-only attack)

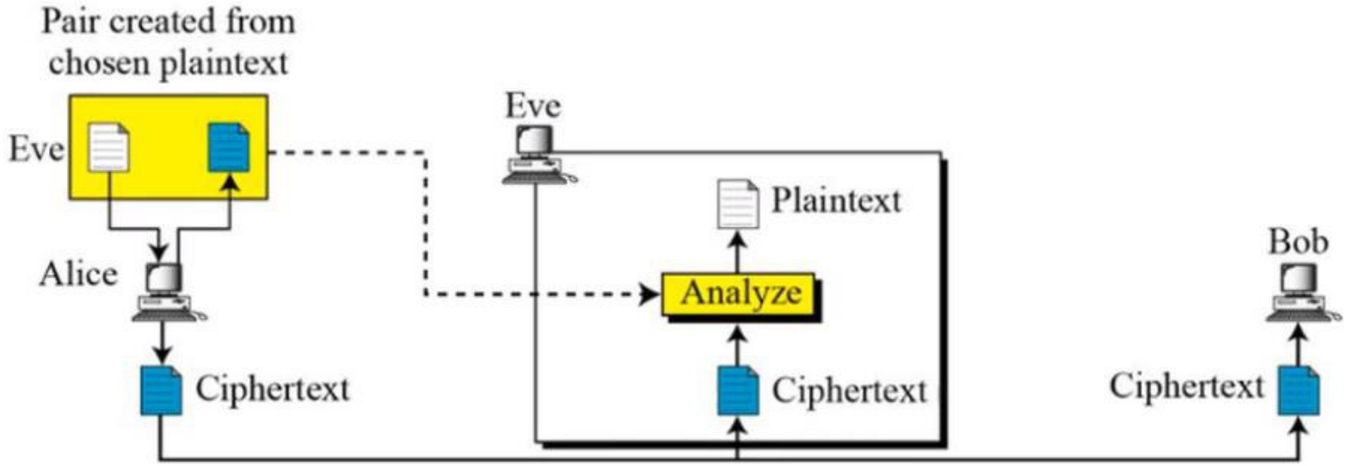
Криптоаналітику відомий алгоритм шифрування і в його розпорядженні є деяка множина перехоплених повідомлень (криптограм), але невідомий секретний ключ.



3. Типи атак на криптосистеми

Атака на основі обраного відкритого тексту (chosen-plaintext attack)

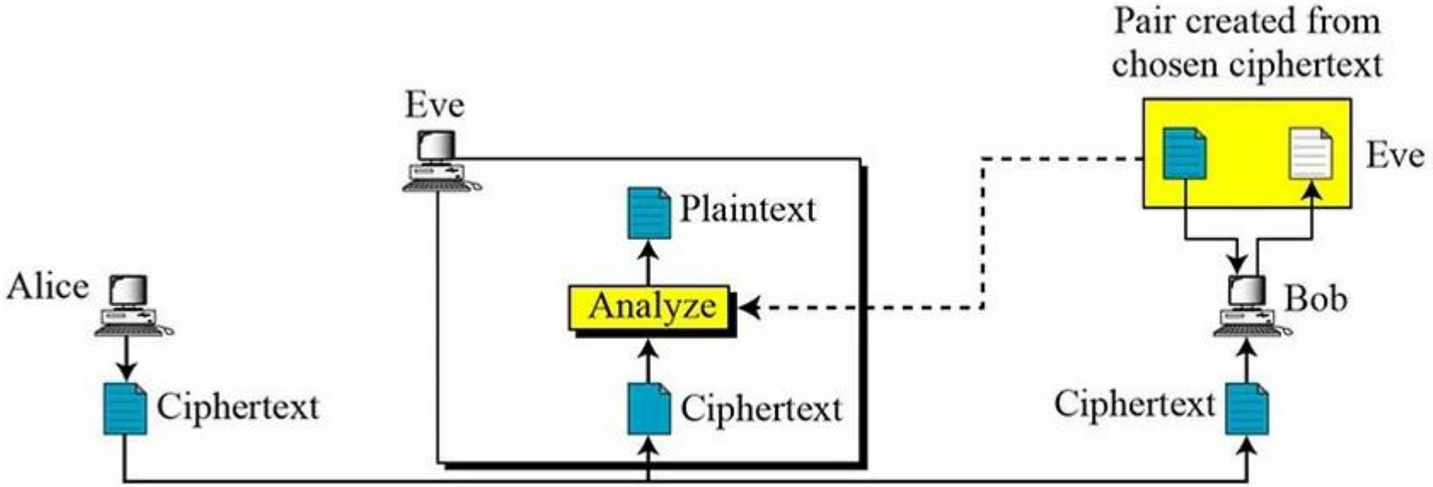
Криптоаналітик володіє певною кількістю відкритих текстів і відповідних шифротекстів, крім того, він має можливість зашифрувати кілька попередньо обраних відкритих текстів.



3. Типи атак на криптосистеми

Атака на основі обраного шифротексту (chosen-cipher attack)

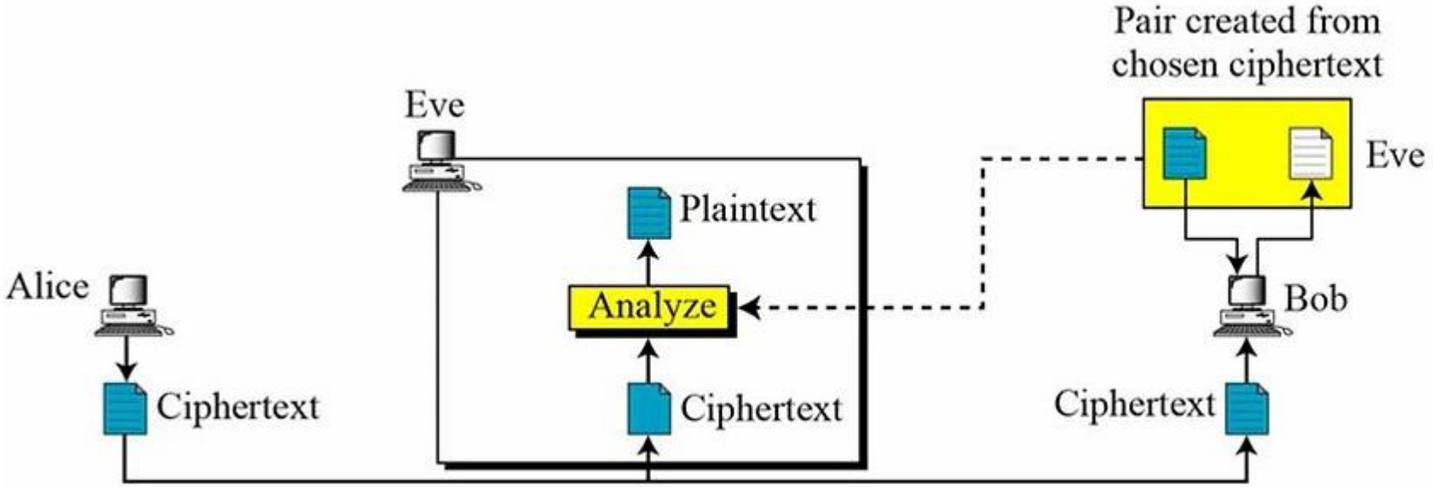
Криптоаналітик збирає інформацію про шифр шляхом підбору зашифрованого тексту. Як правило, криптоаналітик може скористатися пристроєм розшифрування один або кілька разів без знання ключа.



3. Типи атак на криптосистеми

Атака на основі обраного шифротексту (chosen-cipher attack)

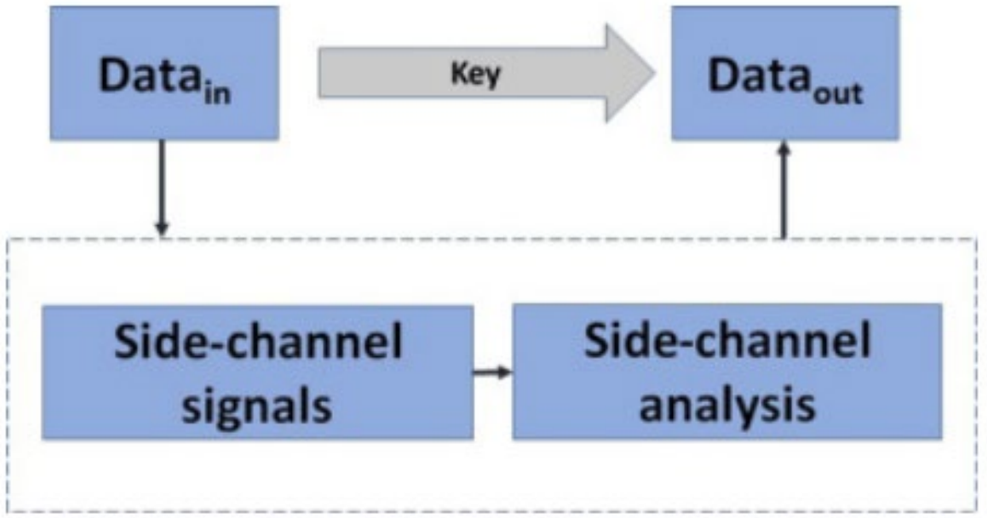
Криптоаналітик збирає інформацію про шифр шляхом підбору зашифрованого тексту. Як правило, криптоаналітик може скористатися пристроєм розшифрування один або кілька разів без знання ключа.



3. Типи атак на криптосистеми

Атака на основі сторонніх каналів (side-channel attacks)

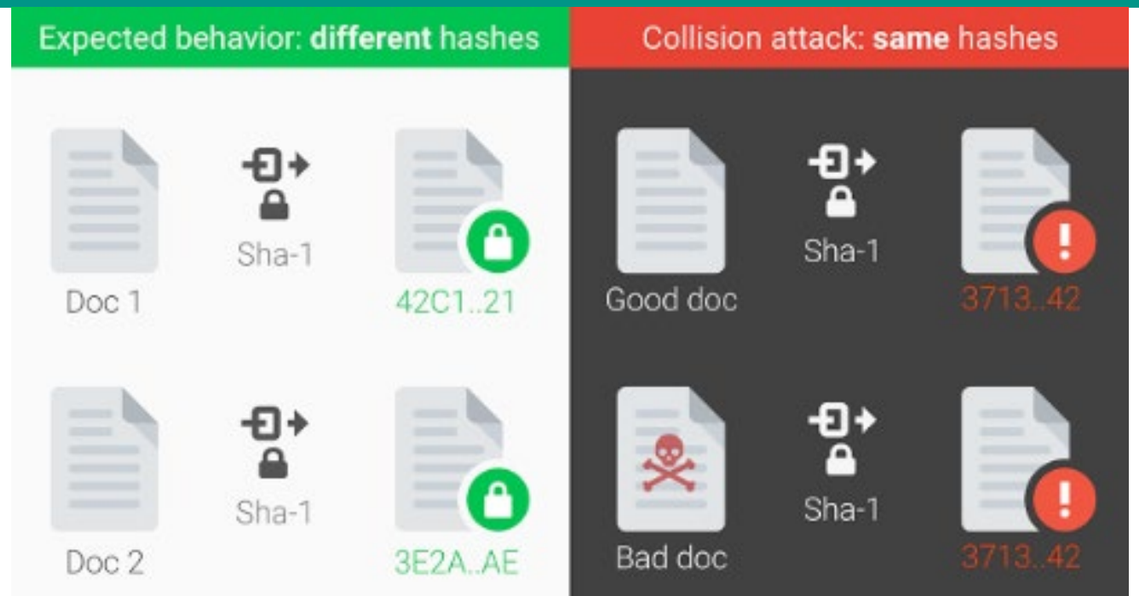
Використовуються не лише математичні особливості алгоритму, а й стороння інформація, як-от час обробки, енергоспоживання і т.д.



3. Типи атак на криптосистеми

Атаки з використанням колізій (collision attacks)

Використовуються у хеш-функціях для пошуку двох різних повідомлень, які дають однаковий хеш. Це може дозволити зловмиснику підробити цифрові підписи або порушити цілісність даних.



3. Типи атак на криптосистеми

Симетричні криптосистеми

- **Криптостійкість** залежить від довжини ключа, складності алгоритму та методів атаки.

Загрози:

атаки методом грубої сили;

диференціальний криптоаналіз;

лінійний криптоаналіз.

Асиметричні криптосистеми

- **Криптостійкість** залежить від складності математичних задач, на яких базується шифрування.

Загрози:

атака методом факторизації;

атака на дискретний логарифм;

квантові комп’ютери.