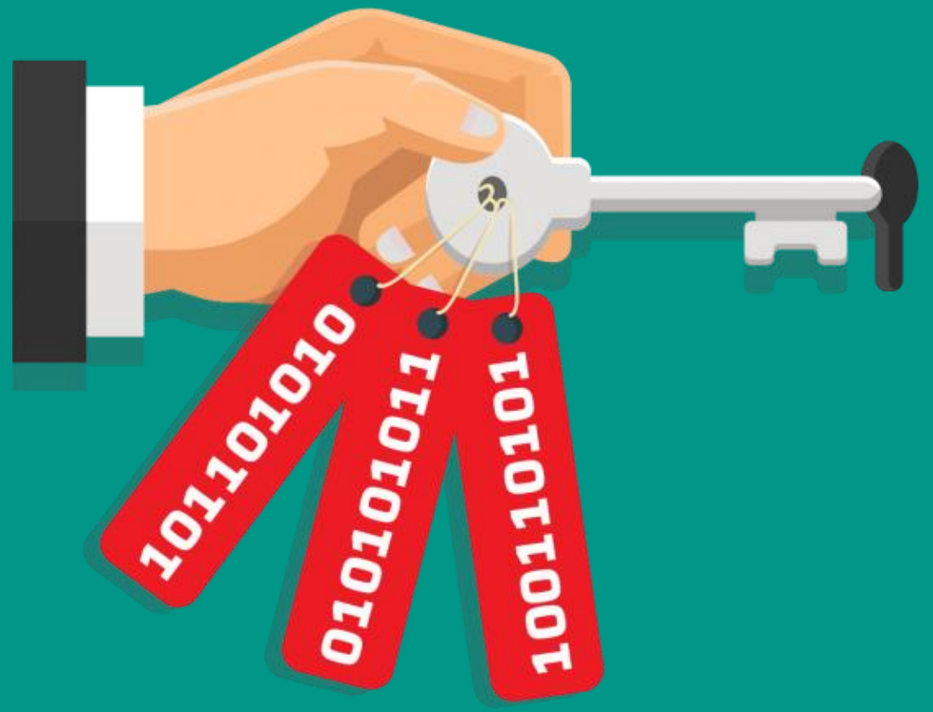
ЛЕКЦІЯ 3

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Криптографічна стійкість шифрів



План

1. Поняття криптографічної стійкості

2. Абсолютно стійкий шифр

3. Типи атак на криптосистеми

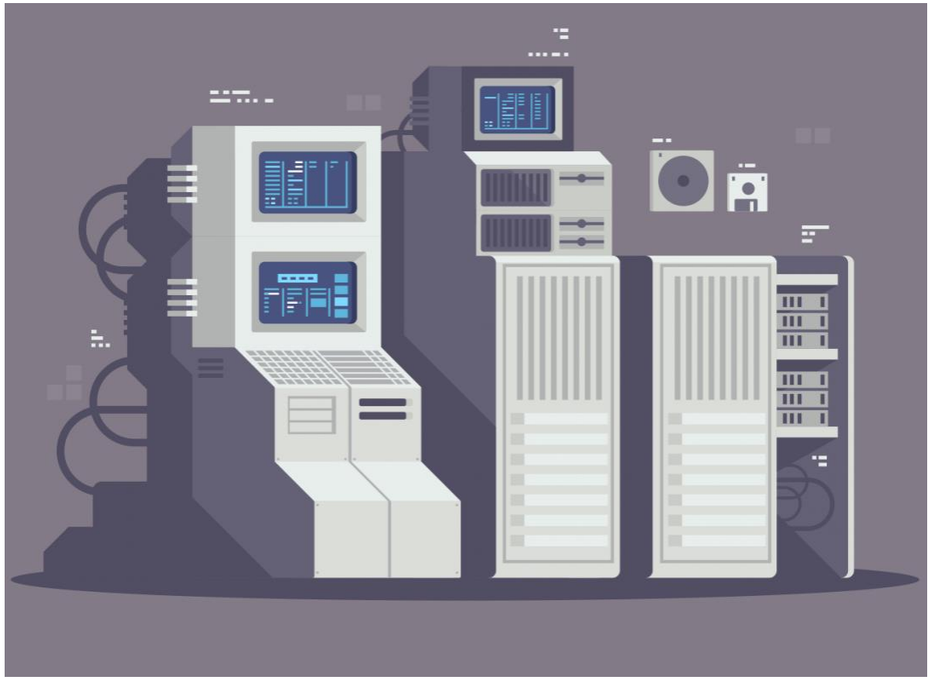
1. Поняття криптографічної стійкості

Криптографічна стійкість – здатність криптографічного алгоритму протидіяти криптографічному аналізу (потенційним атакам супротивника)

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. Розмір ключа, який забезпечує необхідний рівень стійкості. Чим довший ключ, тим складніше зламати криптосистему
2. Час, необхідний для реалізації атаки. Чим більше часу потрібно для успішного зламу системи, тим вищий рівень її стійкості
3. Обчислювальні витрати, необхідні для проведення криптоаналізу. Деякі атаки можуть вимагати значних обчислювальних ресурсів для виконання математичних операцій, таких як факторизація великих чисел або дискретного логарифмування

1. Поняття криптографічної стійкості

Властивості притаманні стійким шифрам

Розсіювання

(Diffusion)

забезпечує поширення впливу окремих символів відкритого тексту на увесь шифротекст (реалізується через перестановку)

Перемішування

(**C**onfusion)

забезпечує поширення впливу окремих символів ключа на увесь шифротекст (реалізується через підстановку (заміну))

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

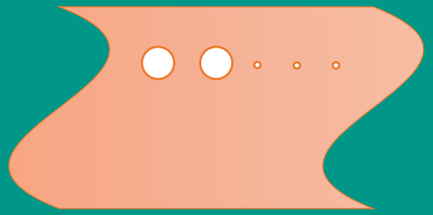
Ідея автоматичного шифрування телеграфних повідомлень

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

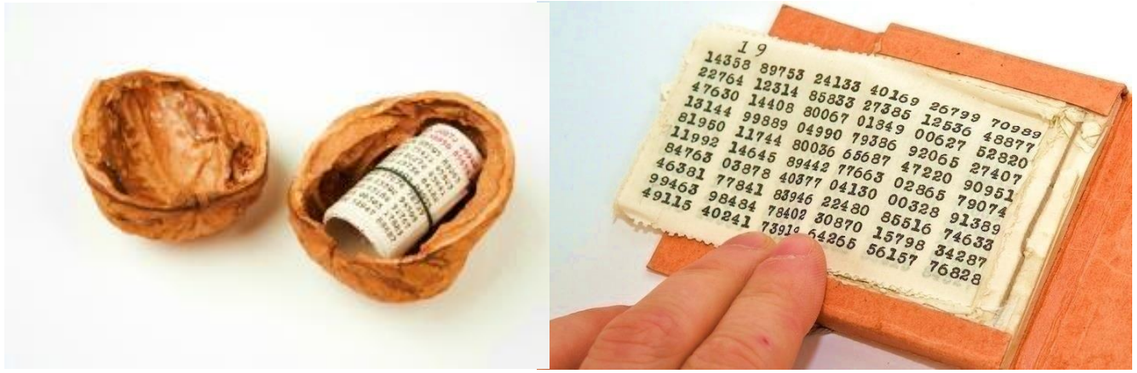
Дешифрування:

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

$\oplus$	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?

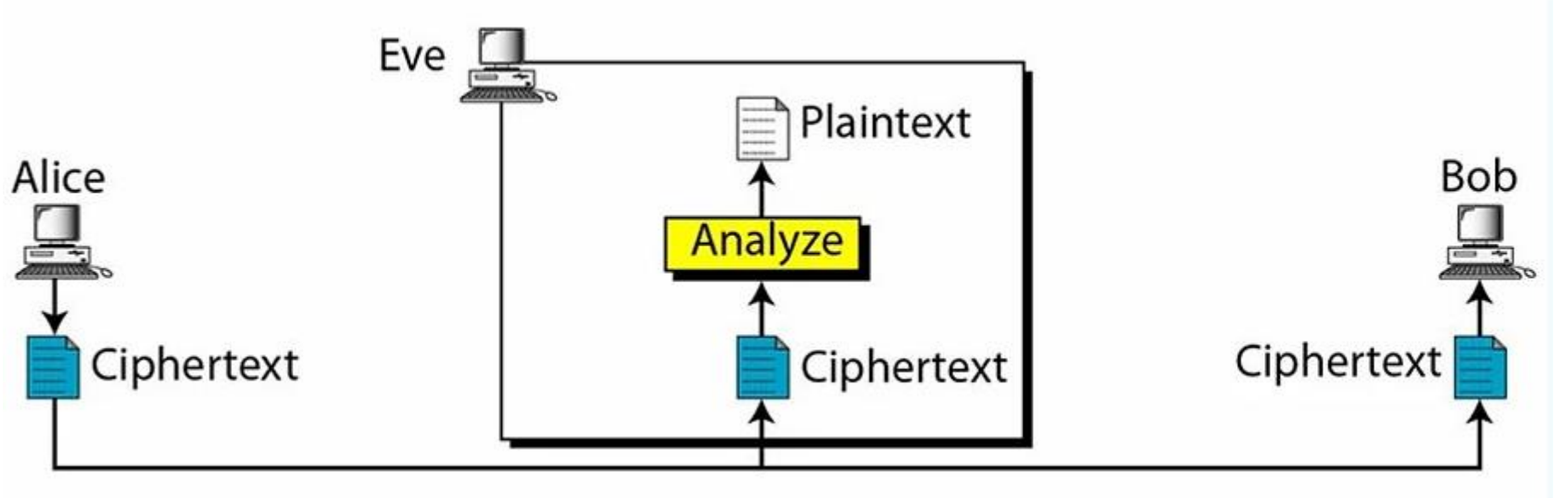
Недоліки:

- ✓ проблема генерації та зберігання ключа;
- ✓ проблема передачі ключа

3. Типи атак на криптосистеми

Атака на основі шифротексту (ciphertext-only attack)

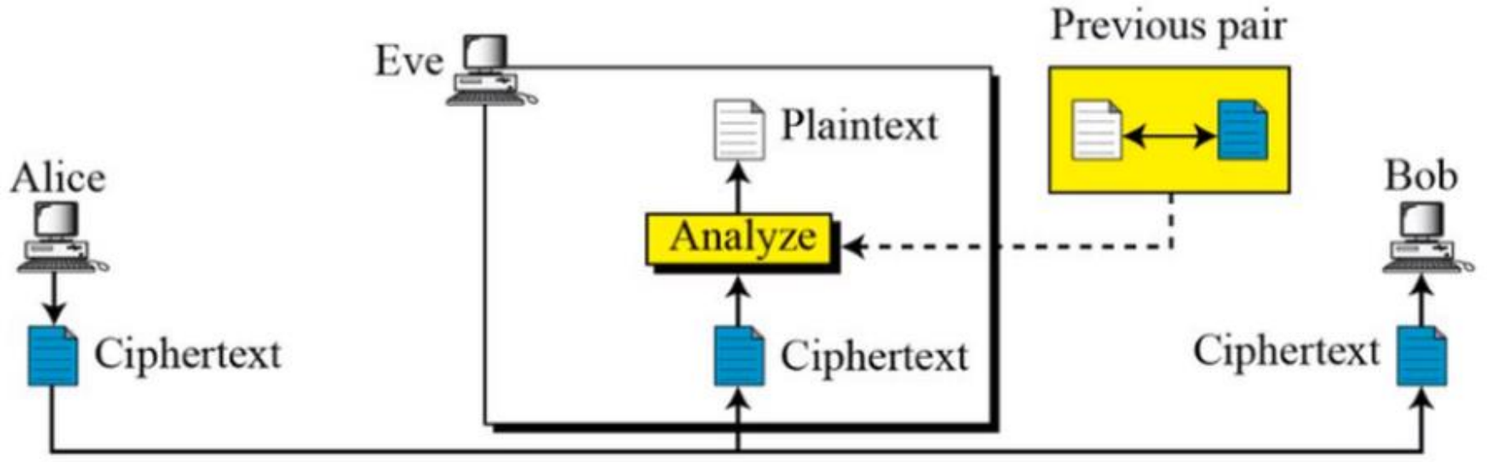
Криптоаналітику відомий алгоритм шифрування і в його розпорядженні є деяка множина перехоплених повідомлень (криптограм), але невідомий секретний ключ



3. Типи атак на криптосистеми

Атака на основі відкритого тексту (known-plaintext attack)

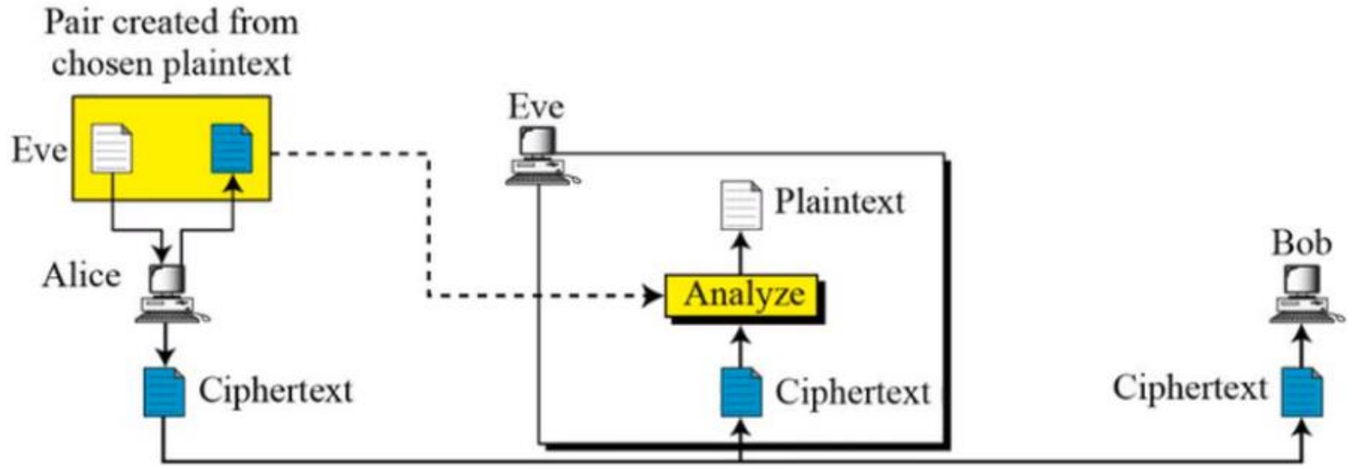
Криптоаналітик має доступ, принаймні, до обмеженої кількості пар відкритого тексту та відповідного шифрованого тексту



3. Типи атак на криптосистеми

Атака на основі 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 може вибрати фрагмент зашифрованого тексту та спробувати отримати відповідний відкритий текст. Як правило, криптоаналітик може скористатися пристроєм розшифрування один або кілька разів без знання ключа