Симетричні криптосистеми

Модифікації DES

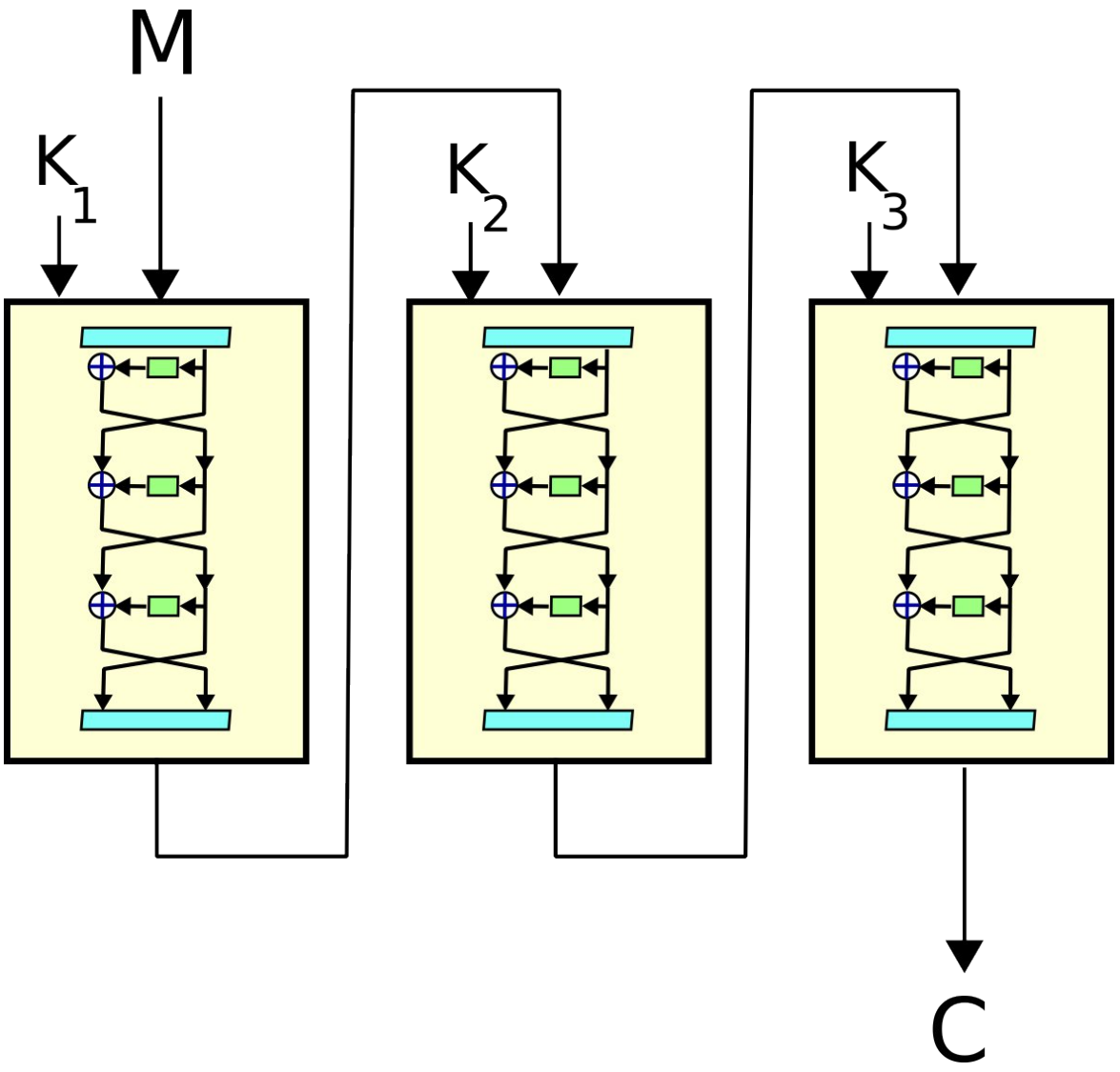
Для чого потрібні модифікації DES?

- Основний недолік алгоритму DES:
  - Мала довжина ключа (64 біти = 56 +8 бітів парності);
- 1997 рік – Distributed NET, атака «грубою силою» на DES - 96 днів;
- 1998 рік – 41 день;
- 1999 рік – 2 дні і 8 годин;
- 1999 рік – 22 години.
- Для подолання малої стійкості алгоритму до атаки грубою силою криптографи пропонували кілька вдосконалень.
- Ми розглянемо 2 з них.

Triple DES (3DES)

- Розробник — IBM, 1978 рік.
- Розробники: У.Діффі, М.Хеллман; У.Тачмен.
- Офіційна назва: TDEA (Triple Data Encryption Algorithm);
- ==========
- Різновиди 3DES:
  - 3DES-EEE3 (використовуються операції шифрування-шифрування-шифрування);
  - 3DES-EDE3 (використовуються операції шифрування-розшифрування-шифрування);
  - 3DES-EEE2 — 3DES-EDE2 (різновиди з двома ключами).

3DES з трьома ключами



- Формальне означення:

$C=3DES_{K1K2K3}(M)$
$=DES(K_3;DES(K_2;DES(K_1;M)));$

3DES з трьома ключами

- 3DES — EEE3 (encryption-encryption-encryption).
- Вхідне повідомлення M шифрується 3 рази на трьох різних ключах:

$C_1=E_{K1}(M)$ $C_2=E_{K2}(C_1)$ $C=E_{K3}(C_2)$

зашифрування

$C_2=D_{K3}(C)$ $C_1=D_{K2}(C_2)$ $M=D_{K1}(C_1)$

розшифрування

3DES з трьома ключами

- 3DES — EDE3 (encryption-decryption-encryption).
- Вхідне повідомлення M шифрується на першому ключі, розшифровується на 2-му і знов шифрується на 3-му:

$C_1 = E_{K1}(M)$ $C_2 = D_{K2}(C_1)$ $C = E_{K3}(C_2)$

зашифрування

$C_2 = D_{K3}(C)$ $C_1 = E_{K2}(C_2)$ $M = D_{K1}(C_1)$

розшифрування

3DES з двома ключами

- 3DES — EEE2 (encryption-encryption-encryption).
- Вхідне повідомлення M шифрується 3 рази на двох різних ключах:

$C_1=E_{K1}(M)$ $C_2=E_{K2}(C_1)$ $C=E_{K1}(C_2)$

зашифрування

$C_2=D_{K1}(C)$ $C_1=D_{K2}(C_2)$ $M=D_{K1}(C_1)$

розшифрування

3DES з двома ключами

- 3DES — EDE2 (encryption-decryption-encryption).
- Вхідне повідомлення M шифрується на першому ключі, розшифровується на 2-му і знов шифрується на 1-му:

$C_1 = E_{K1}(M)$ $C_2 = D_{K2}(C_1)$ $C = E_{K1}(C_2)$

зашифрування

$C_2 = D_{K1}(C)$ $C_1 = E_{K2}(C_2)$ $M = D_{K1}(C_1)$

розшифрування

Переваги та недоліки 3DES

- Велика довжина ключа, а значить, стійкість до атак «грубою силою»:
  - Довжина ключа 3DES з 2-ма ключами: 56+56=112 секретних бітів;
  - Довжина ключа 3DES з 3-ма ключами: 56+56+56=168 бітів;
  - ==========
- Втричі менша швидкодія.
- ==========
- 3DES-EDE3 повністю сумісний з DES, якщо К1=К2=К3.
- 3DES-EDE2 повністю сумісний з DES, якщо К1=К2.

Архітектура 3DES

- Чому використовують конструкцію (2n+1)DES а не 2DES?

Атака «зустріч посередині»

3DES — найшвидша конструкція, стійка до такого типу атак.

DESX

- 1984 року Рональд Рівест (RSA Security) запропонував інший спосіб покращення алгоритму, позбавлений недоліків 3DES.
- Він отримав назву DESX (DES eXtended).
- Формально DESX можна описати так:

$$DESX(M) = K_2 \text{ XOR } DES_K(M \text{ XOR } K_1).$$

- В цьому випадку говорять, що ключі K_1(64 біти) та K_2(64 біти) забілюють повідомлення M. Ключ K (56 бітів) — звичайний ключ DES.
- Загальна довжина ключа 56+64+64 = 184 біти.
- Швидкодія майже така сама, як і у DES (лиш на дві операції XOR більше);
- Існують модифікації де замість XOR використовують додавання за mod 2^{64}.

Висновки

- **Модифікації DES призначені для подолання його основного недоліка: малої довжини ключа.**
- **Найпопулярнішими модифікаціями вважаються:**
  - 3DES-EDE3
  - 3DES-EDE2;
  - DESX.
- **3DES й сьогодні використовується в**