A block cipher with parameters $k$ and $\ell$ is a pair of deterministic algorithms $(E, D)$ such that

- Encryption $E : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$
- Decryption $D : \{0, 1\}^k \times \{0, 1\}^\ell \rightarrow \{0, 1\}^\ell$

Examples:

- 3DES : $\ell = 64$, $k = 56$
- AES : $\ell = 64$, $k = 128, 192, 256$

Wide deployed in banking (ATM machines) and commerce
Each DES Feistel round is invertible

\[
\begin{align*}
48\text{-bit } K_i &+ f R_{i-1} L_{i-1} \\
R_i &+ f R_{i-1} L_{i-1}
\end{align*}
\]

DES: decryption circuit

\[
\begin{align*}
\text{64-bit ciphertext} &+ f \text{ after key expansion} \\
\text{64-bit plaintext}
\end{align*}
\]

DES: the function \(f\)

\[
\begin{align*}
\text{32-bit } X &+ 48\text{-bit } K_i \\
\text{P}
\end{align*}
\]
**DES: S₅-box**

$$ S₅ : \{0, 1\}^6 \to \{0, 1\}^4 $$

(source: Wikipedia)

→ Note that $S₅$ is not reversible as it maps 6 bits to 4 bits.

---

**Attacks on DES**

- **Exhaustive search:** it takes $2^{56}$ to do an exhaustive search over the key space
  → COBACOBANA (120 FPGAs, ~ 10K$): 7 days
- **Linear cryptanalysis:** found affine approximations to DES
  → can find 14 key bits in time $2^{42}$
  → brute force the remaining $56-14=42$ in time $2^{42}$
  ⇒ total attack time $\approx 2^{43}$

⇒ DES is badly broken! Do not use it in new projects!!

---

**Triple DES (3DES)**

- **Goal:** build on top of DES a block cipher resistant against exhaustive search attacks
- **Let DES = (E₅₅, D₅₅). We build 3DES = (E₃₅₅, D₃₅₅) as follows**
  - $E₃₅₅ : (\{0, 1\}^3 × \{0, 1\})^6 \to \{0, 1\}^6$
    - $E₃₅₅((K₁, K₂, K₃), M) = E₅₅(K₁, D₅₅(K₂, E₅₅(K₃, M)))$
    → $K₁ = K₂ = K₃ \Rightarrow$ DES
  - $D₃₅₅ : (\{0, 1\}^3 × \{0, 1\})^6 \to \{0, 1\}^6$
    - $D₃₅₅((K₁, K₂, K₃), C) = D₅₅(K₃, E₅₅(K₂, D₅₅(K₁, C)))$

→ 3 times as slow as DES!!

- **key-size = 3 × 56 = 168 bits**
  → Exhaustive search attack in $2^{168}$

- **simple (meet in the middle) attack in time $2^{118}$**

---

**What about double DES (2DES)?**

- **E₂₅₅((K₁, K₂), M) = E₅₅(K₁, E₅₅(K₂, M))**
  - For $m$ and $c$ such that $E₂₅₅((k₁, k₂), m) = c$ we have that $E₅₅(k₂, m) = D₅₅(k₁, m)$
  → $2₅₅$ admits a meet in the middle attack that reduces the time for key recovery from $2^{112}$ for an exhaustive search to $2^{56}$. Given $M = (m₁, \ldots, m₉)$ and $C = (E₂₅₅((k₁, k₂), m₁), \ldots, E₂₅₅((k₁, k₂), m₉))$
  - For all possible $k₂$, compute $E₅₅(k₂, M)$
  - Sort table according to the resulting $E₅₅(k₂, M)$
  - For each possible $k₁$, compute $D₅₅(k₁, C)$
  - Look up in the table if $D₅₅(k₁, C) = E₅₅(k₂, M)$
  \[ 2^{56}\log(56) \]

⇒ time $< 2^{63}$

- **Similar attack on 3DES in time $2^{118}$**
The Advanced Encryption Standard (AES)

- Goal: replace 3DES which is too slow (3DES is 3 times as slow as DES)
- 2001: NIST adopts Rijndael as AES
- Block size $\ell = 128$ bits, Key size $k = 128, 192, 256$ bits
- AES is Substitution-Permutation network (not a Feistel network)

AES: encryption circuit

- $m_i$: 4 x 4 byte matrix, $K_i$: 128-bit key
- $m_0$: plaintext, $m_{11}$: ciphertext
- at the last round MixColumns is not applied

$\rightarrow$ As AES is not a Feistel network, each step needs to be reversible!

AES: SubBytes

- $\forall j, k. \ m'_i[j, k] = S[m_i[j, k]]$
- rows: most significant 4 bits
- columns: least significant 4 bits

$\rightarrow$ Note that SubBytes is reversible

AES: ShiftRows
**AES: MixColumns**

![AES MixColumns Diagram]

**Attacks on AES**

- **Related-key attack** on the 192-bit and 256-bit versions of AES: exploits the AES key schedule [A. Biryukov, D. Khovratovich (2009)]
  \[\rightarrow\text{key recovery in time } \sim 2^{99}\]

- **First key-recovery attack** on full AES [A. Bogdanov, D. Khovratovich, C. Rechberger (2011)]
  \[\rightarrow4\text{ times faster than exhaustive search}\]

\[\Rightarrow\text{Existing attacks on AES} - 128 \text{ are still not practical, but use AES} - 192 \text{ and AES} - 256 \text{ in new projects!}\]

---

**Using block ciphers**

Myrto Arapinis  
School of Informatics  
University of Edinburgh

**Goal:** Encrypt $M$ using a block cipher operating on blocks of length $\ell$ when $|M| > \ell$
**Electronic Code Book (ECB) mode**

(E, D) a block cipher.

To encrypt message \( M \) under key \( K \) using ECB mode:

- \( M \) is padded:
  \[ M' = M || P \text{ such that } |M'| = m \times \ell \]
- \( M' \) is broken into \( m \) blocks of length \( \ell \):
  \[ M' = M_1 || M_2 || \ldots || M_m \]
- Each block \( M_i \) is encrypted under the key \( K \) using the block cipher
  \[ C_i = E(K, M_i) \text{ for all } i \in \{1, \ldots, m\} \]
- The ciphertext corresponding to \( M \) is the concatenation of the \( C_i \)s
  \[ C = C_1 || C_2 || \ldots || C_m \]

**Weakness of ECB**

\[ m: \quad m_1 \quad m_2 \quad \ldots \quad m_m \]

\[ E_{ECB}(k,m): \quad c_1 \quad c_2 \quad \ldots \quad c_m \]

Problem: \( \forall i, j. \ m_i = m_j \Rightarrow c_i = E(k, m_i) = E(k, m_j) = c_j \)

\[ \Rightarrow \text{Weak to frequency analysis!} \]

\[ \text{\rightarrow PlayStation attack} \]

**Weakness of ECB in pictures**

Original image

Image encrypted using ECB mode

**Cipher-block chaining (CBC) mode: encryption**

(E, D) a block cipher that manipulates blocks of size \( \ell \).

\[
\begin{array}{cccc}
\text{IV} & m_0 & + & m_1 & + & m_2 & + & m_3 \\
\text{IV} & C_0 & E(k,) & C_1 & E(k,) & C_2 & E(k,) & C_3 \\
\end{array}
\]

IV chosen at random in \( \{0,1\}^\ell \)
Cipher-block chaining (CBC) mode: decryption

Counter (CTR) mode

\((E, D)\) a block cipher that manipulates blocks of size \(\ell\).

IV chosen at random in \(\{0, 1\}^\ell\)