DD2448 Foundations of Cryptography

Symetric Cryptosystem

A tuple $(gen, \mathcal{P}, E, E^{-1})$

gen - key generation algorithm outputting $k \in \mathcal{K}$

$\mathcal{P}$ - set of plaintexts

E - deterministic encryption algorithm

E^{-1} - deterministic decryption algorithm

$$E_k^{-1}(E_k(m)) = m \quad \forall m \in \mathcal{P} \quad \forall k \in \mathcal{K}$$

Examples

- Caesar Cipher - shift letter in alphabet by n letters.
  - weak against frequency analysis
- Affine Cipher - multiply & shift
  $c_i = a \cdot m_i + b \bmod m$ a and m are coprime
- Substitution Cipher - Picks a random Permutation and simply switch letters accordingly.

Beaten by frequency analysis by either one or more symbo at the same time.
for example "e" is the most common letter in English. ant "th" is a common pair of letters.

- Vigénère Cipher - Substitute m_i according to a key k_i
  - makes frequency analysis more difficult
- Hill Cipher - K is an invertible matrix over $\mathbb{Z}_{27}$
  $\bar{c} = \bar{m}A \quad \bar{m} = \bar{c}A^{-1}$
  - trivial to breaks if a plaintext pair is known.
- Permutation Cipher - Scramble (transposition) letters order without changeing the letters themselves.
  - special case of Hill Cipher.

Attacks

- Cipher Only
- Known Plaintext
- Chosen Plaintext
- Chosen Ciphertext

Confusion & Diffusion

Confusion - Hide relationship between plain- and cyphertext

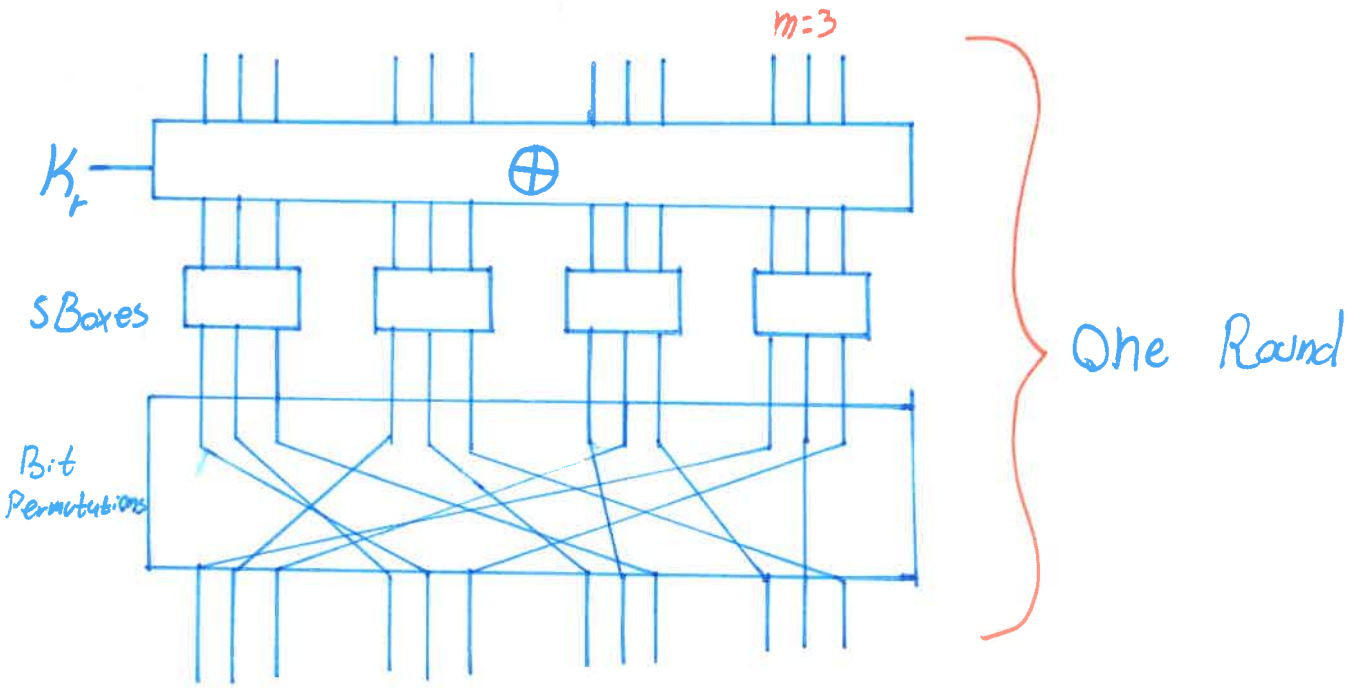
Diffusion - spread changes of cypher out across entire message.

Substitution-Permutation Networks

Block-size $n = l \times m$ bits use r rounds with unique key K_r

Each round

1) Xor with key
2) substitution on m bit words
3) Permutation on the bits.



Advanced Encryption Standard AES

Public competition 1997-2000
Won by Rijmen & Daemen
Key-recovery attack discovered in 2011 that beats brute force by 4x

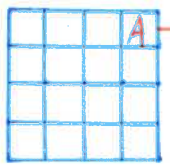
Key bits	128	192	256
Rounds	10	12	14

- Xor round key
- substitute bytes
- Shift rows
- Mix colums

Each step has an inverse operation.

Sub Bytes

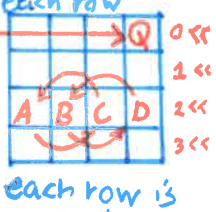
16 bytes = 128 bits



each block is substituted according to a 8 bit Sbox

Shift rows

Cycle blocks in each row

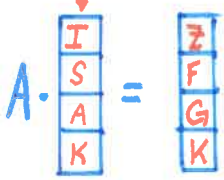


each row is shifted by different amount

Mix Colums

multiply each row by irreducible polynomial

$x^8 + x^4 + x^3 + x + 1$



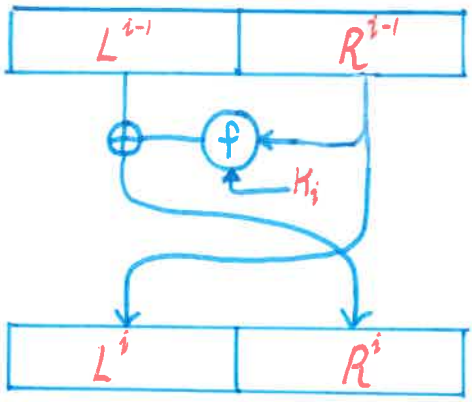
Feistel Network

- Identical Rounds are iterated with different keys
- message is divided into a left and a right part.
- Preimage resistant funktion f that is not invertible
- Each round

$$L_i = R_{i-1} \qquad R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

- ! Invert

$$L^{i-1} = R^i \oplus f(L^i, k^i) \qquad R^{i-1} = L^i$$



Data Encryption Standard DES

Developed at IBM (or NSA) in 1975
16 round feistel network
56 bit key (+8 Parity bits)
Special chip could brute force in 1998
(Probably done by NSA much earlier)

Double DES

One way to increase the keyspace is to run it twice... or is it?

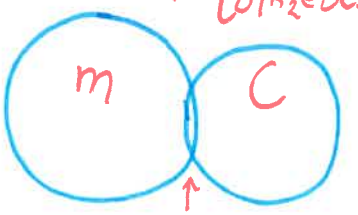
$$2DES_{k_1,k_2}(x) = DES_{k_2}(DES_{k_1}(x))$$

Wrong! Meet in the middle attack

meet in the middle
given a pair (m, c)

build $X = \{x \mid k_1 \in Desk \wedge x = DES_{k_1}(m)\}$

build $Y = \{y \mid k_2 \in Desk \wedge y = DES^{-1}_{k_2}(c)\}$



Very small intersection

Triple DES

This seems secure however, effectively 112 bits.
Very slow however, AES is simply better.

Modes Of Operation

Electronic Codebook Mode

↳ Each block is encrypted independantly

$C_i = E_K(m_i)$

↳ Identical blocks have identical cipher

Cipher Feedback Mode

↳ XOR plaintext with previous cipherblock <u>after</u> encryption.

C_0 = initialization $\quad C_i = m_i \oplus E_K(C_{i-1})$

↳ Sequential encryption, parallel decryption self-synchronizing and unidirectional

Cipher Block Chaining Mode

↳ xor plaintext with previous ciphertext <u>before</u> encryption

C_0 = initialization $\quad C_i = E_K(C_{i-1} \oplus m_i)$

↳ Sequential encryption, parallel decryption

Selfsynchronizing

Output Feedback Mode

↳ Generate stream and xor Plaintext with Stream (one time pad)

S_0 = Stream initialization

$S_i = E_K(S_{i-1}) \quad C_i = S_i \oplus m_i$

↳ Sequential, Synchronous, batch processing

<u>Malleable</u>

Counter Mode

↳ Stream and xor plaintext

S_0 = init

$S_i = E_K(S_0 \| i)$

$C_i = S_i \oplus m_i$

↳ Parallel, Synchronious, batch

<u>malleable</u>

Linear Cryptoanalysis of SPN

Basic Idea

↳ find an expression of the form

$$P_{i_1} \oplus \cdots \oplus P_{i_p} \oplus C_{j_1} \oplus C_{j_c} = K_{l_1 s_1} \oplus \cdots \oplus K_{l_k s_k}$$

with a high probability of occurrence.

↳ Each random plaintext, ciphertext pair gives a hint of

$$K_{l_1 s_1} \oplus \cdots \oplus K_{l_k s_k}$$

↳ Bias Let X be a random binary variable then the bias of X is defined by

$$\varepsilon(X) = P[X=0] - \frac{1}{2}$$

$\Rightarrow \approx \frac{1}{\varepsilon^2(x)}$ samples are required to estimate $P[X=0]$

Linear Approximation of S-Box

Let X and Y be in/out-put of an S-Box. $Y = S(X)$

we then consider bias of their linear combination to be

$$a \cdot X \oplus b \cdot Y = \left(\bigoplus_i a_i X_i\right) \oplus \left(\bigoplus_i b_i Y_i\right)$$

a and b are vectors which determine which bits of X affects b bits of Y

↳ You would expect half of the bits of X to Affect Y but sometimes it is very different

Differential Cryptoanalysis

In short a pair of (Δ, Δ') are searched after such that

$$S(x \oplus \Delta) = S(x) \oplus \Delta'$$

this property can be traised and exploited.

Negligible Function

a function $\varepsilon(n)$ is negligible if $\forall c > 0$ there exists a constant n° such that

$$\varepsilon(n) < \frac{1}{n^c} \qquad \forall n \geq n_0$$

this means f <u>cannot</u> be exploited in polynomial time.

Remaining Notes are Incomplete