4.2. Perfect Secrecy

$\hat{M} \in \mathcal{M}$, $\hat{K} \in \mathcal{K}$ stoch. indep. r.v.

$\hat{C} = e(\hat{M}, \hat{K})$

Def. 4.9. A cryptosystem has perfect secrecy if

$$H(\hat{M} \mid \hat{C}) = H(\hat{M}) . \lrcorner$$

$\Longleftrightarrow$ $\hat{M}, \hat{C}$ are stoch. indep.

- Vernam ciphers have perfect secrecy.

5. Fast Block Ciphers

5.1. The Data Encryption Standard (DES)

- 15. May 1973: NBS (today NIST) solicited proposals for a block cipher. An algorithm from IBM was chosen, based on a predecessor called LUCIFER.
  People involved: Roy Adler, Don Coppersmith, Horst Feistel,
  Alan Konheim, ...
- 17 March 1975: DES was published, public discussion
- 15 Jan. 1977: DES adopted as a standard for unclassified applications.

DES was reviewed each 5 year.
Last official review in Jan. 1999.
Initially expected DES would be standard for 10-15 years.
It proved to be much more durable.

- 19.5.2005 NIST suspended DES as a standard.

5.2.

5.1.1. Key Generation

Key of length 56 bits + 8 parity check bits

$$K_0 = (k_1, \dots, k_7, b_1, k_9, \dots, k_{15}, b_2, \dots, k_{57}, \dots, k_{63}, b_8)$$

From K_0 16 subkeys $K_1, \dots, K_{16}$ are constructed as follows:

- Form 2 blocks of 28 bits each: C_0, D_0 (table 1)
- Construct C_n, D_n from C_{n-1}, D_{n-1} by a cyclic shift by s_n positions with

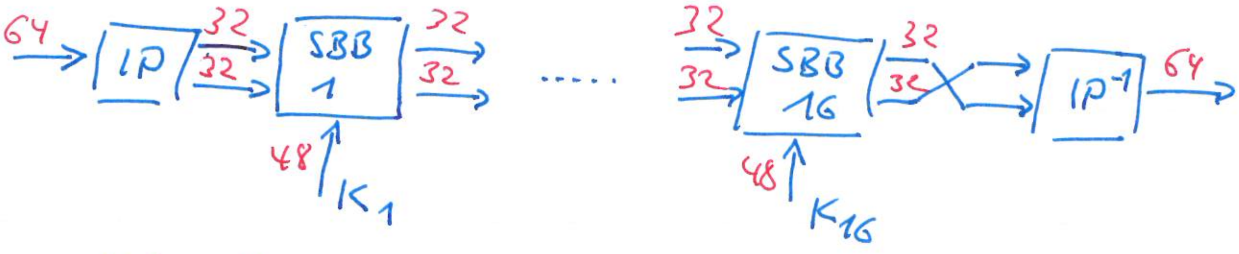
$$s_n = \begin{cases} 1, & \text{if } n \in \{1,2,9,16\} \\ 2, & \text{otherwise} \end{cases}, \quad n = 1, \dots, 16$$

- From each (C_n, D_n) select 48 bits. (table 2)

Each subkey is used in one standard building block. (SBB).

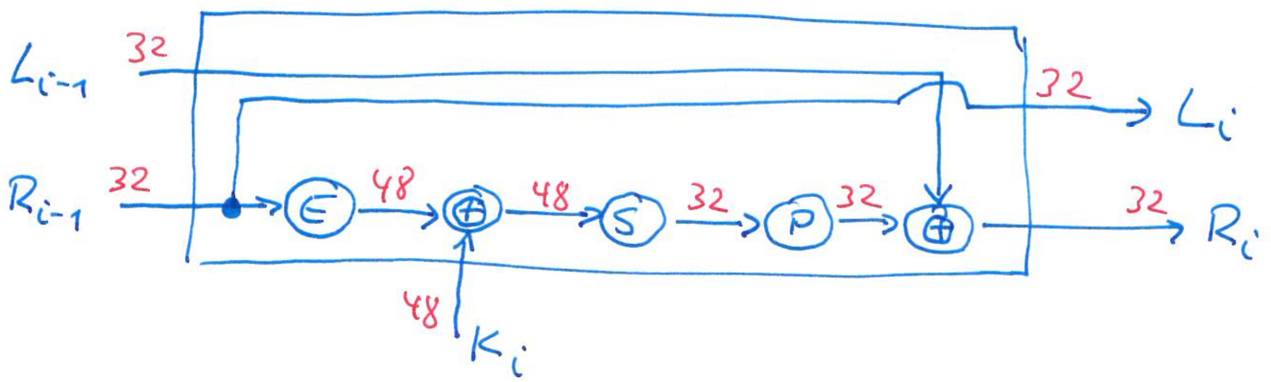
5.1.2. DES Encryption

Plaintext of 64 bits (otherwise group into blocks of 64 bits)



- IP (IP^{-1}): initial permutation (and inverse), splits into 2 blocks of 32 bits (table 3)

- SBB_i :



Formally : $L_i = R_{i-1}$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) , \quad i = 1, \dots, 16$$

E : expansion map, permutation, 16 bits are doubled (table 5)

⊕ : xoring

P : permutation (table 6)

S : transformation $\{0,1\}^{48} \to \{0,1\}^{32}$

48 bits are partitioned into 8 blocks of 6 bits.

$B = (B_1, \dots, B_8)$, $B_i = (b_{i1}, b_{i2}, \dots, b_{i5}, b_{i6})$, $i = 1, \dots, 8$

$$S_i(B_i) = \text{bin}\left(a^{(i)}_{(b_{i1}, b_{i6}), (b_{i2}, \dots, b_{i5})} \right)$$

$a^{(i)}_{kl}$: (k,l)-th entry of S_i (S-boxes)

$$S(B) = (S_1(B_1), \dots, S_8(B_8))$$

Ex. $B_5 = (101010)$ $\quad (10) \mathrel{\hat{=}} 2$

$(0101) \mathrel{\hat{=}} 5$

$$a^{(5)}_{2,5} = 13 \mathrel{\hat{=}} (1101)$$

5.1.3. DES Decryption

It holds $L_i = R_{i-1}$, $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$

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

R_{16}, L_{16} are interchanged in the last step. Hence, the same alg. can be used for decryption with keys $K_{16}, \dots, K_1$ in reverse order.

5.1.4. Security

- Design criteria of the S-boxes have not been published.
- An IBM proposal was modified by NSA.

DES is vulnerable to mainly 2 attacks:

[D. Coppersmith, IBM J. Res. Development, vol. 38, no. 3, May 1994, p. 243-250]

- Differential cryptanalysis [Book: Biham, Spr. 2011]

  S-boxes are optimized against diff. cryptanalysis. Method was known by IBM researchers 20 year ago? Factor 512 faster than brute force = exhaustive search.

- Exhaustive search

  1977: Diffie & Hellman proposed a machine that could break DES in 1 day. Estimated costs US $ 20 million, never built

1998: DES-cracker by EFF
US $ 250'000, appr. 2 days

2006: COPACOBANA (Bochum, Kiel)
120 FPGAS, $ 10'000, 6.4 days for cracking

2008: COPACBANA RIVYERA
less than 1 day.

2016: https:// crack.sh
online tool, promise 25 sec.

5.1.5. Triple DES

Main criticism: key of 56 bits is too short.
Apply DES 3 times with different keys.

2 versions:

Key (K_1, K_2, K_3) (168 bits)

$$c = DES_{K_3}(DES^{-1}_{K_2}(DES_{K_1}(m)))$$

Key (K_1, K_2) (122 bits)

$$c = DES_{K_1}(DES^{-1}_{K_2}(DES_{K_1}(m)))$$

DES^{-1} to ensure compatibility with DES by $K_1 = K_2 = K_3$.