$$H(X) = -\sum_{i=1}^{m} p_i \log p_i \quad , \; p_i = P(X=x_i), \; i=1,\dots,m$$

$$H(X,Y) = -\sum_{i,j} p_{ij} \log p_{ij} \quad , \; p_{ij} = P(X=x_i, Y=y_j)$$

$$H(X|Y) = -\sum_{i,j} P(X=x_i, Y=y_j) \log P(X=x_i | Y=y_j)$$

Th. 4.3.

a) $0 \le H(X) \le \log m$

b) $0 \le H(X|Y) \le H(X)$

c) $H(X) \overset{(i)}{\le} H(X,Y) \overset{(ii)}{\le} H(X) + H(Y)$

"=" in (ii) $\Leftrightarrow$ X, Y are stoch. independent

"=" in (i) $\Leftrightarrow$ $\exists\, P(Y=y_j | X=x_i) = 1$
$\forall i,j : P(X=x_i, Y=y_j) > 0$.

d) $H(X,Y) = H(X) + H(Y|X)$
$= H(Y) + H(X|Y)$ (chain rule)

Proof. Any book on Information Theory.

Shannon:
- $H(X) \le \bar{n}(g)$ for all u.d. codes
  ↑ average code word length (*)
- $\log m$ is the worst case average code word length
- $R = 1 - \frac{H(X)}{\log m}$ is called <u>redundancy</u>.

RWTH AACHEN UNIVERSITY

(*) Take care of log-base and size of alphabet.

4.2. Perfect Secrecy

Cryptosystem $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ with finite sets

$\mathcal{M} = \{M_1, \dots, M_m\}$ messages

$\mathcal{K} = \{K_1, \dots, K_k\}$ keys

$\mathcal{C} = \{C_1, \dots, C_n\}$ ciphertexts

$\hat{M}, \hat{K}$ stoch. indep. r.v. with support $\mathcal{M}, \mathcal{K}$, resp., distribution

$$P(\hat{M} = M_i) = p_i \quad , \quad P(\hat{K} = K_j) = q_j$$

Encryption: $\hat{C} = e(\hat{M}, \hat{K})$ with distribution

$$P(\hat{C} = C_\ell) = r_\ell = \sum_{(i,j):\, e(M_i, K_j) = C_\ell} p_i q_j \quad , \quad \ell = 1, \dots, n$$

Corresponding entropies:

$$H(\hat{M}) = -\sum_i p_i \log p_i \quad , \quad H(\hat{K}) = -\sum_j q_j \log q_j$$

$$H(\hat{C}) = -\sum_\ell r_\ell \log r_\ell$$

$H(\hat{K} \mid \hat{C})$ is called <u>key equivocation</u>

$H(\hat{M} \mid \hat{C})$ is called <u>message equivocation</u>

Thinking the Future
Zukunft denken

<u>Def. 4.9.</u> A cryptosystem $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ is said to have <u>perfect secrecy</u>, if

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

Interpretation: No information about the message is obtained from the ciphertext.

<u>Corollary 4.11.</u> A cryptosystem has perfect secrecy

$\Leftrightarrow$ $\hat{M}$ and $\hat{C}$ are stoch. independent

$\Leftrightarrow P(\hat{M} = M_i \mid \hat{C} = C_l) = P(\hat{M} = M_i) \quad \forall i, l \; P(\hat{C} = C_l) > 0$

$\Leftrightarrow P(\hat{C} = C_l \mid \hat{M} = M_i) = P(\hat{C} = C_l) \quad \forall i, l \; P(\hat{M} = M_i) > 0.$

Tedious to check. Easy sufficient conditions are needed

<u>Th. 4.14.</u> $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ has perfect secrecy if

(i) $P(\hat{K} = K) = \dfrac{1}{|\mathcal{K}|} \quad \forall K \in \mathcal{K}$

(ii) for all $M \in \mathcal{M}, C \in \mathcal{C}$ there is a unique $K \in \mathcal{K}$ such that $e(M, K) = C$.

RWTH AACHEN UNIVERSITY

Proof.

$$P(\hat{C}=C \mid \hat{M}=M) \overset{(ii)}{=} \frac{P(e(\hat{M},\hat{K})=C,\ \hat{M}=M)}{P(\hat{M}=M)}$$

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

$$= P(e(M,\hat{K})=C) \overset{(ii)}{=} P(\hat{K}=K(M,C)) \overset{(i)}{=} \frac{1}{|\mathcal{K}|}$$

Further:

$$P(\hat{C}=C) = \sum_{M\in\mathcal{M}} P(\hat{C}=C \mid \hat{M}=M)\cdot P(\hat{M}=M)$$

$$= \frac{1}{|\mathcal{K}|} \underbrace{\sum_{M\in\mathcal{M}} P(\hat{M}=M)}_{=1} = \frac{1}{|\mathcal{K}|}$$

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

$\underset{\text{Cor. 4.11.}}{\Longrightarrow}$ perfect secrecy $\square$

Vernam ciphers have perfect secrecy.

$\mathcal{X}=\{0,\dots,m-1\}$, $\mathcal{M}_N = \mathcal{C}_N = \mathcal{K}_N = \mathcal{X}^N$

$e(M,K) = ((a_1+s_1) \bmod m, \dots, (a_N+s_N) \bmod m)$

$M=(a_1,\dots,a_N)$, $K=(s_1,\dots,s_N)$

$\hat{M}_N = (\hat{M}_1,\dots,\hat{M}_N)$ r.v. with support $\mathcal{M}_N$

$\hat{K}_N = (\hat{K}_1,\dots,\hat{K}_N)$, $\hat{K}_1,\dots,\hat{K}_N$ i.i.d. $P(\hat{K}_j=i)=\frac{1}{m}$,

$i=1,\dots,m$

RWTH AACHEN UNIVERSITY

Th. 4.15. Vernam cipher has perfect secrecy.

Proof.

(ii) $\forall M \in \mathcal{M}_N, C \in \mathcal{C}_N \; \exists! K \in \mathcal{K}_N : e(M,K) = C$. ✓

(i) $P(\hat{K}_N = K) = P(\hat{K}_1 = s_1, \ldots, \hat{K}_N = s_N)$

$$= \prod_{i=1}^{N} P(\hat{K}_i = s_i) = \frac{1}{m^N} = \frac{1}{|\mathcal{K}_N|}.$$

$\blacksquare$

5. Fast Block Ciphers

5.1. The Data Encryption Standard (DES)

- 1973: Nat. Bureau of Standards (NBS), today Nat. Inst. of Standards and Technology (NIST) solicited proposals for a cryptosystem. An algorithm developed at IBM was chosen, an improvement LUCIFER.
- 1975: DES was published, public discussion started.
- 1977: DES became a standard for unclassified application.
- DES was reviewed every 5 years. Initially it was considered to be secure for 10-15 years. It proved to be more durable
- 2005: NIST suspended DES as a standard.

Thinking the Future
Zukunft denken

5.1.1. Key generation

Key length 56 bits + 8 parity check bits (for error detection)

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

From K_0 16 subkeys $K_1,\dots,K_{16}$ are generated:

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

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

- From each (C_n, D_n) select 48 bits, which are the subkeys $K_1,\dots,K_{16}$.

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