2 Perfect Security

Definition 1 The cipher F is called **perfectly secure** on M_0 (the finite set of all possible plaintexts) if $P(\bullet, c) = P$ on M_0 for all ciphertexts $c \in \Sigma^*$ of positive probability $P(c) > 0$.

Interpretation: This condition assures that the a posteriori probability $P(a|c)$ of each plaintext $a \in M_0$ is the same as the a priori probability $P(a)$. Or in other words, the cryptanalyst doesn't get any additional information on the plaintext by knowing the ciphertext.

Lemma 1 $\#M_0 \leq \#C_0$.

Proof. Let $l \in K$ be a fixed key with $P(l) > 0$. For every ciphertext $c \in f_l(M_0)$, say $c = f_l(b)$, we then have

$$P(c) = \sum_{a \in M_0} P(a) \cdot \sum_{k \in K_{ac}} P(k) \geq P(b) \cdot P(l) > 0.$$

Hence $c \in C_0$. From this follows that $f_l(M_0) \subseteq C_0$. Since f_l is injective also $\#M_0 \leq \#C_0$. $\diamond$

Lemma 2 *If F is perfectly secure, then $K_{ac} \neq \emptyset$ for all $a \in M_0$ and all $c \in C_0$.*

Proof. Assume $K_{ac} = \emptyset$. Then

$$P(c|a) = \sum_{k \in K_{ac}} P(k) = 0.$$

Hence $P(a|c) = 0 \neq P(a)$, contradiction. $\diamond$

Therefore each possible plaintext can be transformed into each possible ciphertext. The next lemma says that the number of keys must be *very* large.

Lemma 3 *If F is perfectly secure, then $\#K \geq \#C_0$.*

Proof. Since $\sum P(a) = 1$, we must have $M_0 \neq \emptyset$. Let $a \in M_0$. Assume $\#K < \#C_0$. Then there exists a $c \in C_0$ with $f_k(a) \neq c$ for every key $k \in K$, whence $K_{ac} = \emptyset$, contradiction. $\diamond$

Theorem 1 [Shannon] *Let F be perfectly secure. Then*

$$\#K \geq \#M_0.$$

That is the number of keys is at least as large as the number of possible plaintexts.

Proof. This follows immediately from Lemmas 1 and 3. $\diamond$

Theorem 2 [SHANNON] *Let F be a cipher with*

$$P(k) = \frac{1}{\#K} \quad \text{for all } k \in K$$

(that is all keys have the same probability) and

$$\#K_{ac} = s \quad \text{for all } a \in M_0 \text{ and all } c \in C_0.$$

with a fixed $s \geq 1$. Then F is perfectly secure. Furthermore $\#K = s \cdot \#C_0$.

Proof. Let $c \in C_0$ be a possible cipherext. Then for any possible plaintext $a \in M_0$:

$$\begin{aligned} P(c|a) &= \sum_{k \in K_{ac}} \frac{1}{\#K} = \frac{\#K_{ac}}{\#K} = \frac{s}{\#K}, \\ P(c) &= \sum_{a \in M_0} P(a) \cdot P(c|a) = \frac{s}{\#K} \cdot \sum_{a \in M_0} P(a) = \frac{s}{\#K} = P(c|a), \\ P(a|c) &= \frac{P(c|a)}{P(c)} \cdot P(a) = P(a). \end{aligned}$$

Therefore F is perfectly secure. The second statement follows from

$$K = \dot{\bigcup_{c \in C_0}} K_{ac}$$

for all $a \in M_0$. $\diamond$