Shannon's Theory of Secrecy Systems

See:

C. E. Shannon,
Communication Theory of Secrecy Systems, Bell Systems Technical Journal,
Vol. 28, pp. 656–715, 1948.

Notation

Given a cryptosystem, denote

$\boldsymbol{M}$ a message (plaintext)

$\boldsymbol{C}$ a ciphertext

$\boldsymbol{K}$ a key

$\boldsymbol{E}$ be the encryption function $\boldsymbol{C = E_K(M)}$

$\boldsymbol{D}$ be the decryption function $\boldsymbol{M = D_K(C)}$

For any key K, $E_K(\cdot)$ and $D_K(\cdot)$ are 1-1, and $D_K(E_K(\cdot))$ =Identity.

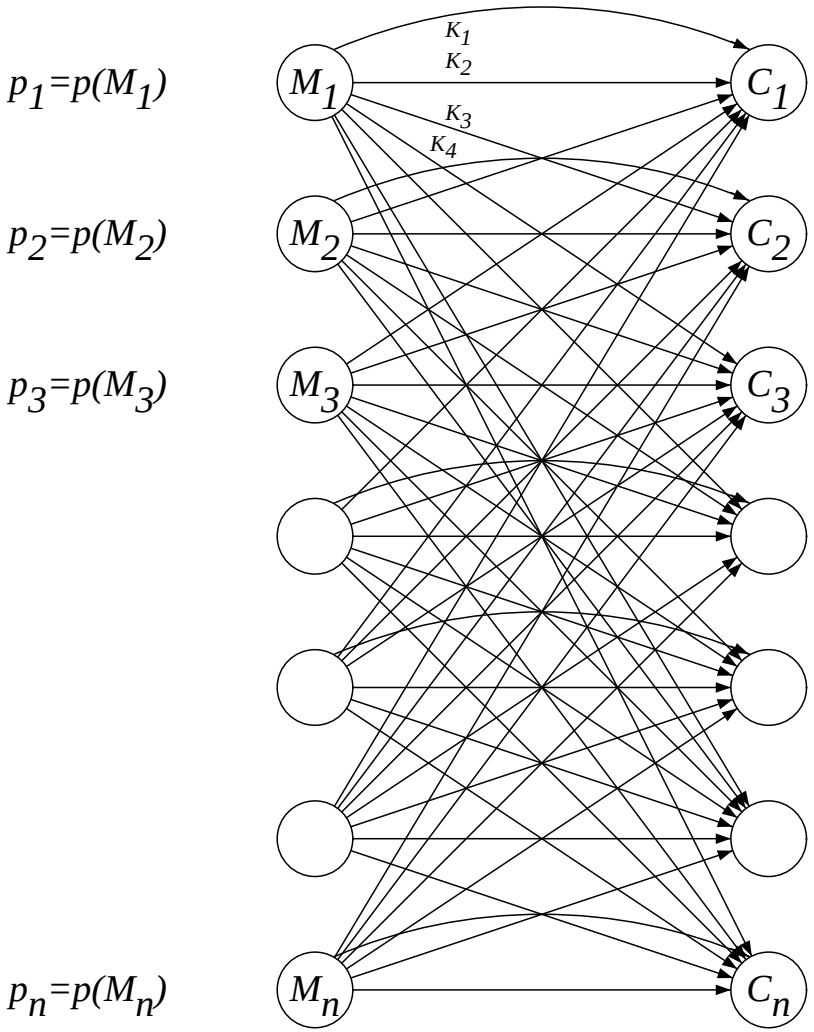
Shannon's Theory of Secrecy Systems (1949)

Let $\{M_1, M_2, \ldots, M_n\}$ be the message space.
The messages $M_1, M_2, \ldots, M_n$ are distributed with known probabilities $p(M_1), p(M_2), \ldots, p(M_n)$ (not necessarily uniform).

Let $\{K_1, K_2, \ldots, K_l\}$ be the key space. The keys $K_1, K_2, \ldots, K_l$ are distributed with known probabilities $p(K_1), p(K_2), \ldots, p(K_l)$. Usually (but not necessarily) the keys are uniformly distributed: $p(K_i) = 1/l$.

Each key projects all the messages onto all the ciphertexts, giving a bipartite graph:

Shannon's Theory of Secrecy Systems (1949) (cont.)



Perfect Ciphers

Definition: A cipher is **perfect** (מושלם) if for any M, C

$$p(M|C) = p(M)$$

(i.e., the ciphertext does not reveal any information on the plaintext).

By this definition, a perfect cipher is immune against ciphertext only attacks, even if the attacker has infinite computational power (unconditional security in context of ciphertext only attacks).

Note that

$$p(M)p(C|M) = p(M,C) = p(C)p(M|C).$$

Perfect Ciphers (cont.)

and thus it follows that

Theorem: A cipher is perfect iff

$$\forall M, C \quad p(C) = p(C|M).$$

Note that

$$p(C|M) = \sum_{\substack{K \\ E_K(M)=C}} p(K).$$

Therefore, a cipher is perfect iff

$$\forall C \quad \left(\sum_{\substack{K \\ E_K(M)=C}} p(K) \text{ is independent of } M \right)$$

Perfect Ciphers (cont.)

Theorem: A perfect cipher satisfies $l \geq n$ (#keys $\geq$ #messages).

Proof: Assume the contrary: $l < n$. Let C_0 be such that $p(C_0) > 0$. There exist l_0 $(1 \leq l_0 \leq l)$ messages M such that $M = D_K(C_0)$ for some K. Let M_0 be a message not of the form $D_K(C_0)$ (there exist $n - l_0$ such messages). Thus,

$$p(C_0|M_0) = \sum_{\substack{K \\ E_K(M_0)=C_0}} p(K) = \sum_{K \in \emptyset} p(K) = 0$$

but in a perfect cipher

$$p(C_0|M_0) = p(C_0) > 0.$$

Contradiction. QED

Perfect Ciphers (cont.)

Example: Encrypting only one letter by Caesar cipher: $l = n = 26$, $p(C) = p(C|M) = 1/26$.

But:

When encrypting two letters: $l = 26$, $n = 26^2$, $p(C) = 1/26^2$.

Each M has only 26 possible values for C, and thus for those C's: $p(C|M) = 1/26$, while for the others C's $p(C|M) = 0$.

In particular, $p(C = XY|M = aa) = 0$ for any $X \neq Y$.

Vernam is a Perfect Cipher

Theorem: Vernam is a perfect cipher.

Vernam is a Vigenere with keys as long as the message. Clearly, if the keys are even slightly shorter, the cipher is not perfect.

Informally, in Vernam cipher, for each possible ciphertext, all the messages are still possible, as given P and C, there is a unique key that encrypts P to C. As we do not have any information on the key (and the keys are selected with uniform distribution), we cannot discard any possible message-key pairs.

Proof: Clearly, in Vernam $l = n$. Given that the keys are uniformly selected at random, $p(K) = 1/l = 1/n$.

$$p(C|M) = p(K = C - M) = \frac{1}{n} = \frac{1}{l}.$$

Since $p(C|M) = 1/l$ for any M and C, clearly also $p(C|M) = p(C)$. QED

This proof hold also in the binary (XOR) case of one-time-pad.

Long Message Encryption

To encrypt a long message $M = M_1 M_2 \ldots M_N$ (M is the full message, the M_i's are the various letters) we encrypt each block M_i to $C_i = E_K(M_i)$ under the same key K, and concatenate the results $C = C_1 C_2 \ldots C_N$.

This cipher is not perfect since there is N such that #keys $<$ #messages of length N (and since $p(XY|aa) = 0 \neq p(XY)$ when $X \neq Y$).

Thus, we can gain information on the key or the message given the ciphertext only (for a given C there are only #keys possible messages, rather than #messages).

Unicity Distance

How long should M and C be so we can identify the message M uniquely given the ciphertext C?

We will instead ask the question: How long should M and C be so we can identify the key K uniquely given the ciphertext C?

We will assume appropriate randomness and independence assumptions on the cipher (i.e., all keys generate different and independent permutations, etc.)

Let H be the average entropy of a plaintext character. It is known that in English $H = 1.5$, i.e., it is possible in theory to compress each character in 1.5 bits, and the approximate number of legal English texts of length m characters is $(2^{1.5})^m$.

Let D be the number of bits of redundancy that each character contains in the plaintext. In English $D = \log 26 - H = 4.7 - 1.5 = 3.2$, i.e., 3.2 bits are redundant in each character. In an ASCII byte, $D = \log 256 - H = 8 - H$.

Unicity Distance (cont.)

Definition: **the unicity distance N** (מרחק היחידות) is

$$N = \frac{\text{key length in bits}}{D}$$

If $D = 0$ an attacker cannot identify the message uniquely. In this case we say that $\boldsymbol{N = \infty}$.

Conclusion: Compression of a message before encrypting reduces D (because the same text is compressed to a shorter length), and thus increases the unicity distance.

Random Ciphers

Assume that the message space and the ciphertext space are of size n (i.e., there are n different messages of size N).

The messages are **redundant**, i.e., not all the n messages are legal, or not all have the same probabilities.

Each key represents a random permutation of the letters, each with probability $1/n!$.

Random Ciphers (cont.)

Example: In English $D = \log 26 - H$. $\log 26 = 4.7$, $H = 1.5$ (as letters are dependent in English). $D = \log 26 - H = 4.7 - 1.5 = 3.2$.

In Caesar's cipher (26 possible shifts), the unicity distance is thus

$$N = \frac{H(K)}{3.2} = \frac{\log 26}{3.2} = 1.5$$

where $H(K)$ represents the key size in bits.

In a substitution cipher

$$N = \frac{H(K)}{3.2} = \frac{\log 26!}{3.2} = \frac{88.4}{3.2} = 27.6$$

In a uniformly random letter distribution, whose frequencies are as in English, $D = 4.7 - 4 = 0.7$ and the unicity distances would be 7 and 126, respectively.