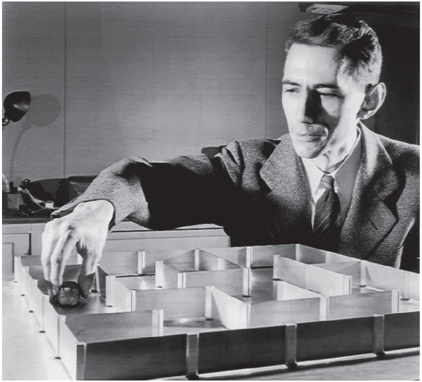
Perfect Secrecy



Claude Elwood Shannon

- Claude Elwood Shannon (1916-2001) was an American mathematician, electronic engineer, and cryptographer — he is known as "The father of Information Theory"
- Two landmark papers he had written established the foundations of information theory and modern cryptography
- He is also credited with founding digital circuit design theory in 1937, when as a 21-year old master's degree student at MIT, he wrote his thesis demonstrating the applications of boolean algebra to construct digital circuits — this work is considered as the most important master's thesis of all times!
- Shannon established the concept of perfect secrecy in his 1948-paper "Communication Theory of Secrecy Systems" (*Bell Systems Technical Journal*, vol 28, pages 656-715)

Shannon's Theory of Secrecy

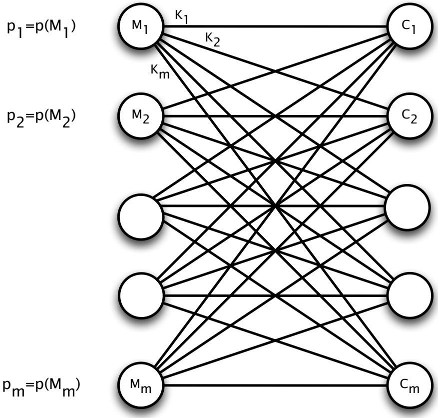
- Consider the block cipher encryption and decryption functions

$$C = E_K(M) \quad \text{and} \quad M = D_K(C)$$

  such that for any key K, the functions $E(\cdot)$ and $D(\cdot)$ are one-to-one, and $D_K(E_K(\cdot))$ is the identity transformation
- Let $\{M_1, M_2, \ldots, M_m\}$ be the message space, where the probability $p(M_i)$ of each message is known a priori, which are not necessarily equal (uniform distribution is not assumed)
- Let $\{K_1, K_2, \ldots, K_k\}$ be the key space, where probability of each key is known as $p(K_i)$, which are usually equal: $p(K_i) = 1/k$ for $i = 1, 2, \ldots, k$ (keys are uniformly distributed)

Bipartite Graph of Mapping

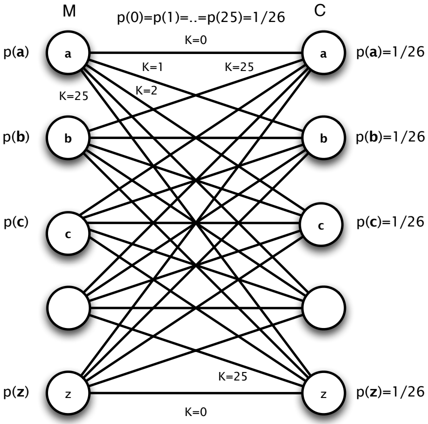
- Keys map all messages to all ciphertexts, giving a bipartite graph



Shift Cipher

- The message space $\{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\}$ and $m = 26$, such that the messages are encoded as integers from $\mathcal{Z}_{26} = \{0, 1, 2, \ldots, 25\}$
- The message probabilities are determined by the language of the communication, and not necessarily equal, for example $p(\mathtt{a}) = 0.082$, $p(\mathtt{e}) = 0.127$, $p(\mathtt{z}) = 0.001$, however $\sum p(M) = 1$
- The key space $\mathcal{Z}_{26} = \{0, 1, 2, \ldots, 25\}$ and $k = 26$, such that a key K is uniformly selected from $\mathcal{Z}_{26}$, and thus, $p(K) = 1/26$
- Any message, for example $M = \mathtt{e}$, is encrypted to any of the ciphertexts $C \in \{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\}$, based on the value of the key: $C = M + K \pmod{26}$
- Since each key $K \in \mathcal{Z}_{26}$ is equally likely, each ciphertext $C \in \{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\}$ is equally likely for a given, fixed message, i.e., $p(C) = 1/26$

Shift Cipher Bipartite Graph



Affine Cipher

- The message space $\{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\}$ and $m = 26$; similarly, the messages are encoded as integers from $\mathcal{Z}_{26} = \{0, 1, 2, \ldots, 25\}$ and the message probabilities are known a priori
- A message, for example $M = \mathtt{e}$, is encrypted to any of the ciphertexts $C \in \{\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\}$, based on the value of the key pair (α, β), via the encryption function $C = \alpha \cdot M + \beta \pmod{26}$
- The key space (α, β) with $\alpha \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$ and $\beta \in \mathcal{Z}_{26}$, and therefore, $k = 12 \cdot 26 = 312$
- The number of keys is more than the number of messages $k > m$
- We also assume that a key K is uniformly selected: $p(K) = 1/312$

Affine Cipher

- There are 312 keys (more than the number of ciphertexts), and thus, a ciphertext C will appear more than once in the encryption of a given, fixed message M
- There are different key pairs (α_1, β_1) and (α_2, β_2) that map the same plaintext to the same ciphertext: $\alpha_1 M + \beta_1 = \alpha_2 M + \beta_2 \pmod{26}$
- For example, for the plaintext $M = \texttt{e}$, the following 12 key pairs (α, β) computes the ciphertext as $C = \texttt{d}$

$$\begin{array}{cccccc} (1,25) & (3,17) & (5,9) & (7,1) & (9,19) & (11,11) \\ (15,21) & (17,13) & (19,5) & (21,23) & (23,15) & (25,7) \end{array}$$

In fact, each of the 26 ciphertexts appears exactly 12 times, therefore, for a given, fixed message each ciphertext is equally likely, as all 312 key pairs are scanned, $p(C) = 12/312 = 1/26$

Perfect Cipher

- A cipher is perfect if for any pair (M, C), the probability of M is equal to the probability of M with the corresponding C is known

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

- This implies that the knowledge of ciphertext does not yield information about the plaintext
- A perfect cipher is immune against ciphertext only attacks
- Even if the adversary has infinite computational power, he/she cannot discover the plaintext in a ciphertext only attack scenario — this is called unconditional security in the context of ciphertext only attacks

Perfect Cipher

- Consider the Bayes' theorem: $p(M)p(C|M) = p(C)p(M|C)$
- Therefore, a cipher is perfect if and only if

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

- Since we have

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

  Therefore, a cipher is perfect if and only

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

Perfect Cipher

- Theorem: For a perfect cipher $k \geq m$, that the number of keys is larger than or equal to the number of messages
- Proof: Assume $k < m$ and consider a ciphertex C^* such that $p(C^*) > 0$. There exists L messages (where $1 \leq L \leq m$) such that $M = D_K(C^*)$ for some K. Let M^* not obtainable from $D_K(C^*)$ (there are $m - L$ such messages), then

$$p(C^*|M^*) = \sum_{\substack{K \\ E_K(M^*)=C^*}} p(K) = \sum_{K \in \emptyset} p(K) = 0$$

This is a contradiction since in a perfect cipher we must have

$$p(C^*|M^*) = p(C^*) > 0$$

Shift Cipher

- Consider the shift cipher for $M \in \{a, b, \ldots, z\}$ for mapping a single letter
- We have 26 keys and 26 messages: $k = m = 26$, and

$$p(C) = p(C|M) = 1/26$$

- When we encrypt 2 letters, we have $k = 26$, and $n = 26^2$, and thus, $p(C) = 1/26^2$
- This implies each M has only 26 values for C, and thus, for those Cs: $p(C|M) = 1/26$, while for the other Cs: $p(C|M) = 0$
- In particular, $p(C = XY|M = aa) = 0$ for any $X \neq Y$

Vernam Cipher

- Vernam cipher is a generalization of the Vigenere cipher, where the key is as long as the message
- Assuming $k = m$ and the keys are selected randomly, we have $p(K) = 1/k = 1/m$, and thus

$$p(C|M) = p(K = C - M) = \frac{1}{m} = \frac{1}{k}$$

  Since $p(C|M) = 1/m$ for any pair (M, C), therefore, $p(C|M) = p(C)$
- For all possible ciphertext, all messages are possible, as given M and C, there is a unique key that encrypts M to C

One-Time Pad

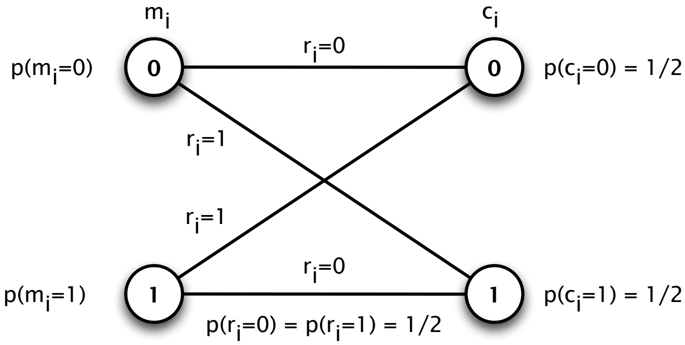
- Vernam cipher is called one-time pad when M, C, K are single bits, and r_i is randomly generated with uniform probability $p(r_i) = 1/2$

$$
\begin{array}{cccc|c|cc}
 & r_1 & r_2 & \cdots & r_i & \cdots & r_n \\
\oplus & m_1 & m_2 & \cdots & m_i & \cdots & m_n \\
\hline
 & c_1 & c_2 & \cdots & c_i & \cdots & c_n
\end{array}
$$

- The message $m_i \in \{0, 1\}$ probabilities $p(0)$ and $p(1)$ may or may not be known, however, they are not assumed to be equal, but $p(0) + p(1) = 1$
- For every value of $c_i \in \{0, 1\}$, there are 2 messages and 2 keys:
  $c_i = 0$ implies $(r_i, m_i) = (0, 0)$ or $(r_i, m_i) = (1, 1)$
  $c_i = 1$ implies $(r_i, m_i) = (0, 1)$ or $(r_i, m_i) = (1, 0)$

One-Time Pad Bipartite Graph

$$p(c_i = 0|m_i = 0) = p(r_i = 0) = 1/2 \quad \text{and} \quad p(c_i = 0|m_i = 1) = p(r_i = 1) = 1/2$$
$$p(c_i = 1|m_i = 0) = p(r_i = 1) = 1/2 \quad \text{and} \quad p(c_i = 1|m_i = 1) = p(r_0 = 1) = 1/2$$



3-bit One-Time Pad

- Similarly, consider the 3-bit ciphertext $(c_1 c_2 c_3)$: this ciphertext was obtained by a bitwise XOR operation of the 3-bit plaintext $(m_1 m_2 m_3)$ and the 3-bit random key $(r_1 r_2 r_3)$ such that $c_i = m_i \oplus r_i$
- The 3-bit key $(r_1 r_2 r_3)$ is one of the following 8 values, with equal $1/8$ probability: $\{000, 001, 010, 011, 100, 101, 110, 111\}$
- We may or may not know the plaintext probabilities, however, each $(m_1 m_2 m_3)$ appears with some probability $0 < p(m_1 m_2 m_3) < 1$
- Regardless of what the plaintext is, each ciphertext is equally likely, with probability $1/8$, for example, if $(m_1 m_2 m_3) = (101)$ then, any of these 8 key and ciphertext pairs are equally likely:

$$\begin{array}{rcccccccc} r_1 r_2 r_3: & 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\ c_1 c_2 c_3: & 101 & 100 & 111 & 110 & 001 & 000 & 011 & 010 \end{array}$$

Electronic Codebook Mode

- Given a long message $M = M_1 M_2 \cdots M_N$, we encrypt each block M_i to $C_i = E_K(M_i)$ using the same key, and append the individual ciphertexts to obtain the result $C = C_1 C_2 \cdots C_N$
- This does not constitute a perfect cipher since for $N > 1$, the number of keys $<$ the number of messages
- Note that $p(C = XY | M = aa) = 0$, however, $p(C = XY) \neq 0$ when $X \neq Y$
- Thus, we can gain some information on the key or the message under a ciphertext only scenario