One-Time Pad

A classic example of a perfectly secure encryption scheme is the one-time pad.

Definition: One-time pad (OTP)

Let the message space $\mathcal{M}$ be some additive group $(G, +)$. Define the random variable K to be uniformly distributed over the key space $\mathcal{K} = \mathcal{M}$, and define the ciphertext space to be $\mathcal{C} = \mathcal{M}$ as well. Define the encryption and decryption function as follows:

$$\begin{aligned} Enc(m,k) &= m + k = c, \\ Dec(c,k) &= c - k = m. \end{aligned}$$

Here, $c - k$ stands for $c + (-k)$, where $-k$ is the additive inverse of k in the group $(G, +)$.

Example: One-time pad for binary strings

The most common use of the one-time pad is for the group of binary strings under (bit-wise) addition modulo 2, i.e. $(\{0,1\}^n, \oplus)$. In this group, every element is its own additive inverse, resulting in the encryption and decryption functions

$$\begin{aligned} Enc(m,k) &= m \oplus k = c, \\ Dec(c,k) &= c \oplus k = m. \end{aligned}$$

For example, if $n = 4$, a possible message m is 0101, and a possible key k is 0110. The ciphertext c is $0101 \oplus 0110 = 0011$, and the decryption of c is again $0011 \oplus 0110 = 0101$, the original message m.

We can show that the one-time pad indeed satisfies the definition of perfect security.

Theorem

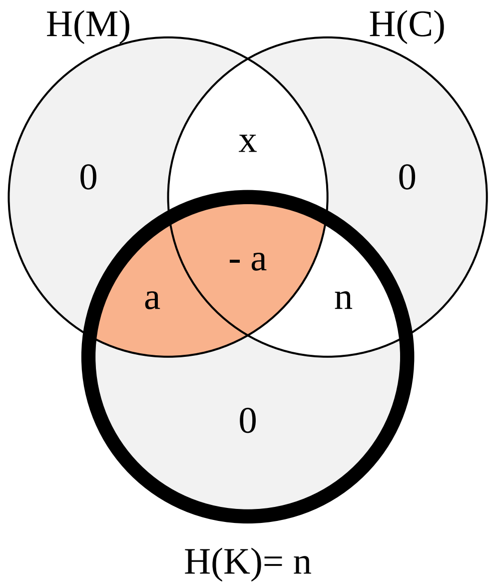
The one-time pad is perfectly secure.

Proof hint

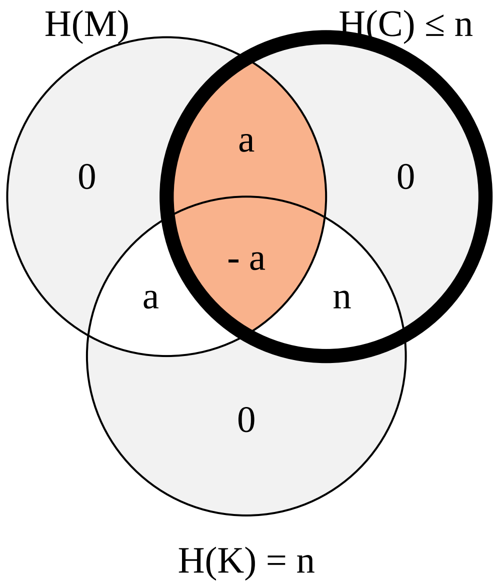
Draw a three-variable entropy diagram for the random variables M, K, and C. Use the fact that the key$K$ is picked uniformly at random, and the setup assumption that it is independent from the message M. Then deduce from the diagram that $I(M;C) = 0$, i.e., the message and ciphertext share no information.

Show full proof

Write $n = \log|G|$. We need to verify that $I(M;C) = 0$. We do so using a three-variable entropy diagram. We can already fill in the values $H(K) = n = \log|G|$ (because K is uniformly distributed), $H(M|CK) = H(C|MK) = H(K|MC) = 0$ (because each random variable is a function of the other two), and $I(M;K) = 0$ (this is our setup assumption).



Note that the area of $I(M;K) = I(M;K|C) + R(M;K;C)$ (shaded orange in the picture) as a whole is 0, but that does not mean that $I(M;K|C)$ and $R(M;K;C)$ themselves are zero, because $R(M;K;C)$ can be negative. We can conclude that there must be some (non-negative) real number $a \geq 0$ such that $I(M;K|C) = a$ and $R(M;K;C) = -a$. As the entropy of K has to be $H(K) = n$, we can furthermore conclude that $I(K;C|M) = n$. From $I(M;C) \geq 0$ follows that $x \geq a$, and because $H(C) \leq n$, it follows that $x \leq a$ and hence, $x = a$ and $I(M;C) = 0$, as desired.



We have thus seen that the one-time pad provides perfect information-theoretic security. There is one enormous drawback to this encryption scheme though: the key needs to be as large as the message! To send a message of n bits, Alice needs to share n bits of key with Bob. It might be tempting for Alice to reuse the key k

for several messages once she has shared it with Bob, but this is dangerous: Eve could, from two intercepted encryptions $(m_1 + k)$ and $(m_2 + k)$, recover the difference of the two plaintext messages $m_1 + k - (m_2 + k) = m_1 - m_2$. Already the difference between two plaintext messages can reveal a lot of information about the individual messages, as illustrated in this Cryptosmith blog post.