POIS-3

10/01/2023 (Tue)

Shannon's Perfect Secrecy

Encryption Schemes are a 4-tuple

$$< Gen, Enc, Dec, M >$$

Gen=Key generation algorithm, will give the key, to the sender and reciever , and is chosen over some distribution over the keyspace.
Enc=Takes the input as the key and the message text, and gives us the cipher text as the output.
Dec=Takes the input as the key and the cipher text, and gives us the message text as the output.
M= The message space.

We do not need all three- message space, key space, and cipher space, we just need one of them, and *Enc*,*Dec*,*Gen* to determine the other two.

An encryption scheme is said to be "perfectly secret" if for all probability distribution over M, Then for all messages, and for all possible ciphertexts c

$$P\left[Message = M \mid ciphertext = c\right] = P\left[Message = M\right]$$

That is, looking at the cipher text, does not give extra information about the message.

Is the Shift Cipher Perfectly Secret?

Gen= Key randomly chosen from the set $\{0, 1, \ldots 25\}$
$Enc \implies c = m + k \bmod 26$
$Dec \implies c = m - k \bmod 26$
$M = \{0, 1, \ldots 26\}^m$

Consider the message string was just "abc" then the Probability of the message being "abc" is $\frac{1}{26^3}$
However, assuming that the encryption scheme is public, then given that the output string is some "xyz", the message string is "abc" is $\frac{1}{26}$. Therefore the shift cipher not perfectly secret. However for extremely small message space, that is for 1 message bit, the algorithm is perfectly secure, since both the probabilities is $\frac{1}{26}$

One-time Pad (Vernum Cipher)

$M = \{0,1\}^m$
$Gen \implies k = \{0,1\}^m$
$Enc \implies c = k \otimes m$
$Dec \implies m = k \otimes c$

The Decryption algorithm works because $m = k \otimes c = k \otimes k \otimes m = m$

Showing the One-time Pad is perfectly secure

We first provide an alternative definition for the perfect secret encryption scheme.
For some probability distribution m, for all ciphertext, and for all message texts

$$P\left[Ciphertext = c \mid message = m\right] = P\left[Ciphertext = c\right]$$

We can also use this to create the **indisinguishiblity condition**

$$P\left[Ciphertext = c \mid mesaage = m_1\right] = P\left[Ciphertext = c \mid mesaage = m_2\right]$$

For all messages m_1, m_2 and for all ciphertexts c.

Proof that the two definitions are equal

We use the Bayes Theorem

$$P\left[A \mid B\right] = \frac{P[B \mid A]P(A)}{P(B)}$$

Now

$$P(Mes = m \mid Cip = c) = P(Mes = m)$$

$$\frac{P(Cip = c \mid Mes = m)P(Mes = M)}{P(Cip = c)} = P(Mes = m)$$

$$P(Cip = c \mid Mes = m) = P(Cip = c)$$

Proving the indistinguishibility condition is straightforward from the above definition, since the rhs does not depend on the message at all.

Proving the other way around (from the indistinguishibility condition to the alternative definition)

$$P(Cip = c) = \sum_{m \epsilon M} P(Cip = c \mid Mes = m)P(Mes = m)$$
$$P(Cip = c) = \sum_{m \epsilon M} a \cdot P(Mes = m) \text{ (indistinguishibility criteria)}$$
$$P(Cip = c) = a \sum_{m \epsilon M} P(Mes = m) = a \cdot 1 = a = P(Cip = c \mid Mes = m)$$

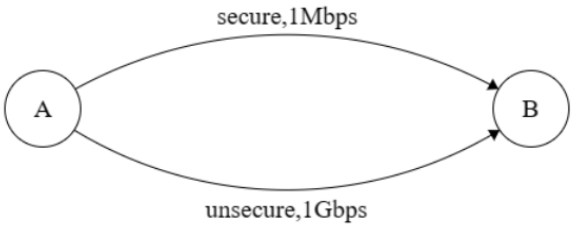
One-Time Pad Proof

$$P(Ciphertext = c \mid message = M) = P(M \otimes K = c \mid M = m)$$
$$= P(m \otimes K = c)$$
$$= P(K = m \otimes c) = 2^{-l}$$

Also since the distribution over the Cipherspace is unform, therefore the value of $P(Ciphertext = c) = 2^{-l}$

Limitation of One-Time Pad

- Consider Communication between A and B, there are two channels, one of which is secure, which is used to send the key, and the other one is insecure, which is used to send the message after encryption. However, assume that the secure channel is slower than the insecure channel. Since the size of the key is the same as the size of the message, we have to wait for the key to be sent before we can actually decrypt, this causes a huge bottleneck.



  For the scheme above, consider a message of size 1Gb. In this scheme even though the message is sent in 1 second, the key takes 1024 seconds to travel, therefore we need to wait for 1024 seconds in order to be able to decrypt the message.

- As the name suggests, the One-Time Pad, is suitable for one time use only. Any subsequent uses, can leak information

$$c_1 \otimes c_2 = m_1 \otimes m_2 \quad \text{(Reveals information about the messages)}$$

The Problem of creating a *slow secure channel, from no secure channel* , is a problem in **public-key cryptography**. And the problem of creating a *fast secure channel from slow secure channel*, is a problem in **symmetric key cryptography**.

Limitations of perfectly secure scheme

In any perfectly secure encryption scheme, the size of the message space, and the size of key space are related as

$$|M| \leq |K|$$

Proof

Lite ig later, can check from the modern cryptography book, basically proof by contradiction.

This would mean that the problem we were facing with one-time pad, will be present in every perfectly secure scheme, that is the rate of transfer will be limited by the bottleneck caused by the rate of the secure channel used to transfer the key