


Shannon's Theory

Debdeep Mukhopadhyay
IIT Kharagpur



Objectives

- Understand the definition of Perfect Secrecy
 - Prove that a given crypto-system is perfectly secured
 - One Time Pad
-



Unconditional Security

- Concerns the security of cryptosystems when the adversary has unbounded computational power, that is has infinite resources.
 - Cipher-text only Attack: Attack the cipher using the cipher texts only.
 - When is a cipher is unconditionally secured?
-



A priori and *A posteriori* Probabilities

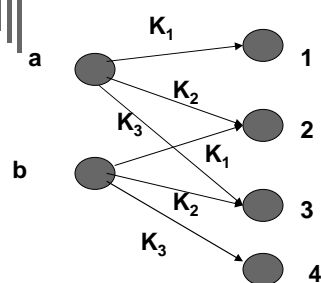
- The plain-text has a probability distribution
 - $p_P(x)$: A priori probability of a plain text
 - The key also has a probability distribution
 - $p_K(K)$: A priori probability of the key.
 - The cipher text is generated by applying the encryption function. Thus $y=e_K(x)$ is the cipher text.
 - Note, that the plain text and the key are independent distributions.
-

Attacker wants to compute a posteriori probability of plain text

- The probability distributions on P and K , induce a probability distribution on C , the cipher text.
- For a key K , $C_K(x) = \{e_K(x) : x \in P\}$
- Does the cipher text leak information about the plain text?

Given, the cipher text y , we shall compute the a posteriori probability of the plain text, ie. $p_P(x|y)$ and see whether it matches with that of the a priori probability of the plain text.

Example



	a	b
K_1	1	2
K_2	2	3
K_3	3	4

- $P = \{a, b\}$; $p_P(a) = 1/4$, $p_P(b) = 3/4$
- $K = \{K_1, K_2, K_3\}$, $p_K(K_1) = 1/2$, $p_K(K_2) = p_K(K_3) = 1/4$
- $C = \{1, 2, 3, 4\}$. What are the a posteriori probabilities of the plain text, given the cipher texts from C ?

Example

$P=\{a,b\}; p_P(a)=1/4,$
 $p_P(b)=3/4$
 $K=\{K_1,K_2\}, p_K(K_1)=1/2,$
 $p_K(K_2)= p_K(K_3)=1/4$

$p_C(1)=p_P(a)p_K(K_1)$
 $= (1/4) \cdot (1/2) = 1/8$

$p_C(3)=p_P(a)p_K(K_3) + p_P(b)$
 $p_K(K_2)$
 $= (1/4)(1/4) + (3/4)(1/4) = 1/16 + 3/16 = 1/4$

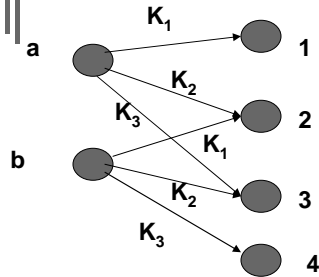
Likewise I can compute the other probabilities...

Example

$P=\{a,b\}; p_P(a)=1/4,$
 $p_P(b)=3/4$
 $K=\{K_1,K_2\}, p_K(K_1)=1/2,$
 $p_K(K_2)= p_K(K_3)=1/4$

- $p_P(a|1)=1; p_P(b|1)=0$
- $p_P(a|2)=?$
- The '2' can come when the plain text was 'a' and the key was 'K₂' or when the plain text was 'b' and the key was 'K₁'
- Given '2', we need to compute the probability that it came from 'a'.
- Is it that of choosing K₂? No.

Example



$P = \{a, b\}$; $p_P(a) = 1/4$,
 $p_P(b) = 3/4$
 $K = \{K_1, K_2, K_3\}$, $p_K(K_1) = 1/2$,
 $p_K(K_2) = p_K(K_3) = 1/4$

- Given '2', we need to compute the probability that it came from 'a'.
- The '2' can appear with a probability:
 - by having 'a' as the PT and K_2 as the key: $(1/4)(1/4) = 1/16$
 - by having 'b' as the PT and K_1 as the key: $(3/4)(1/2) = 6/16$
- $p_P(a|2) = (1/16) / (7/16) = 1/7$


Generalization of the Example

$$p_P(x|y) = \frac{p_P(x) \sum_{K: x=d_K(y)} p_K(K)}{\sum_{\{K: y \in C(K)\}} p_K(K) p_P(d_K(y))}$$



Perfect Secrecy

- A Cryptosystem has perfect secrecy if $p_P(x|y) = p_P(x)$ for all $x \in P, y \in C$.
 - That is the a posteriori probability that the plaintext is x , given that the ciphertext y is observed, is identical to the a priori probability that the plaintext is x .
-



Shift Cipher has perfect secrecy

- Suppose the 26 keys in the Shift Cipher are used with equal probability $1/26$. Then for any plain text distribution, the Shift Cipher has perfect secrecy.
 - Note that $P=K=C=\mathbb{Z}_{26}$ and for $0 \leq k \leq 25$
 - Encryption function: $y = e_k(x) = (x+k) \bmod 26$
-

Perfect Secrecy

$$p_P(x|y) = \frac{p_P(x)p_C(y|x)}{p_C(y)}$$

$$\begin{aligned} p_C(y) &= \sum_{K \in \mathbb{Z}_{26}} p_K(K) p_P(d_K(y)) \\ &= \sum_{K \in \mathbb{Z}_{26}} \frac{1}{26} p_P(y - K) = \frac{1}{26} \end{aligned}$$

$$\begin{aligned} p_C(y|x) &= P_K(y - x \bmod 26) \\ &= \frac{1}{26} \end{aligned}$$

Hence Proved

Theorem

- Suppose (P, C, K, E, D) be a cryptosystem, where $|K|=|C|=|P|$. The cryptosystem offers perfect secrecy if and only if every key is used with probability $1/|K|$, and for every $x \in P$ and every $y \in C$, there is a unique key, such that $y = e_K(x)$.
- Perfect Secrecy (equivalent): $p_C(y|x) = p_C(y)$
 - Thus if Perfect Secret, a scheme has to follow the above equation.



Cryptographic Properties

- $p_C(y|x) > 0$
- This means that for every cipher text, there is a key, K , st. $y = E_K(x)$
- Thus $|K| \geq |C|$. In our case, $|K| = |C|$
- Thus, there is no cipher text, y , for which there are two keys which take them to the same plaintext.
- There is exactly one key, such that $y = E_K(x)$



One-time Pad

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Encryption: Plaintext \oplus Key = Ciphertext

	h	e	i	l	h	i	t	l	e	r
Plaintext:	001	000	010	100	001	010	111	100	000	101
Key:	111	101	110	101	111	100	000	101	110	000
Ciphertext:	110	101	100	001	110	110	111	001	110	101
	s	r	l	h	s	s	t	h	s	r



One-time Pad

Suppose a wrong key is used to decrypt:

	s	r	l	h	s	s	t	h	s	r
Ciphertext:	110	101	100	001	110	110	111	001	110	101
"key":	101	111	000	101	111	100	000	101	110	000
<hr/>										
"Plaintext":	011	010	100	100	001	010	111	100	000	101
	k	i	l	l	h	i	t	l	e	r

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111



One-time Pad

And this is the correct key:

	s	r	l	h	s	s	t	h	s	r
Ciphertext:	110	101	100	001	110	110	111	001	110	101
"Key":	111	101	000	011	101	110	001	011	101	101
<hr/>										
"Plaintext":	001	000	100	010	011	000	110	010	011	000
	h	e	l	i	k	e	s	i	k	e

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111



Unconditionally secured scheme

For a given ciphertext of same size as the plaintext, there is a equi-probable key that produces it. Thus the scheme is unconditionally secured.



Practical Problems

- Large quantities of random keys are necessary.
 - Increases the problem of key distribution.
 - Thus we will continue to search for ciphers where one key can be used to encrypt a large string of data and still provide computational security.
 - Like DES (Data Encryption Standard)
-



One-time Pad Summary

- Provably secure, when used correctly
 - Cipher-text provides no information about plaintext
 - All plaintexts are equally likely
 - Pad must be random, used only once
 - Pad is known only by sender and receiver
 - Pad is same size as message
 - No assurance of message integrity
 - Why not distribute message the same way as the pad?
-



Assignment 1

- Let n be a positive integer. A Latin square of order n is an $n \times n$ array L with integers $1, 2, \dots, n$ such that every integer occurs exactly once in each row and column. An example for $n=3$ is:

1	2	3
3	1	2
2	3	1



Assignment 1

- Given any Latin square of order n , we can define a related cryptosystem, $e_i(j)=L(i,j)$, where $1 \leq i, j \leq n$.

Prove **from the computation of probabilities** that the Latin square cryptosystem achieves perfect secrecy.
