References

- Introduction to Modern Cryptography
  - Katz-Lindell
  - Chapter 2, Perfectly Secret Encryption

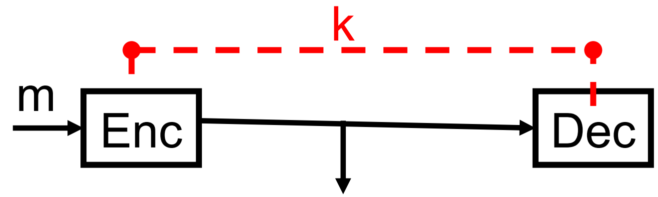
- Cryptography, Theory and Practice
  - Stinson
  - Chapter 1: Classical Cryptography
  - Chapter 2: Shannon’s theory

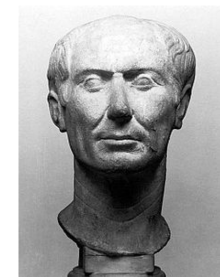
Plan

- Motivation and background
- Measure of secrecy
- Perfect secrecy
  - Requirements – long key
- ε-secrecy
  - Entropy
  - Statistical distance
  - Game-based definition

Information Theoretic Cryptography: *Confidentiality*

- The oldest records from Julius Caesar (~100 BC)
- Symmetric key





Wikipedia

- Caesar cipher:
  - {a,b,c…z} → {0,1,..25}
  - Key = 3
  - 3 + plaintext mod 26
  - Ciphertext - 3 mod26
  - Julius→ MXOLXV

- One-time-pad
  - Gilbert Vernam - Joseph Mauborge : 1917
  - Stream cipher
    - Teletype+ tape

Confidentiality *(Shannon 1949)*

- Goal: Message can only be seen by intended receiver

- Sender and receiver have a shared secret key

  Enc (key, plaintext) =ciphertext

  Dec (key, ciphertext) = plaintext

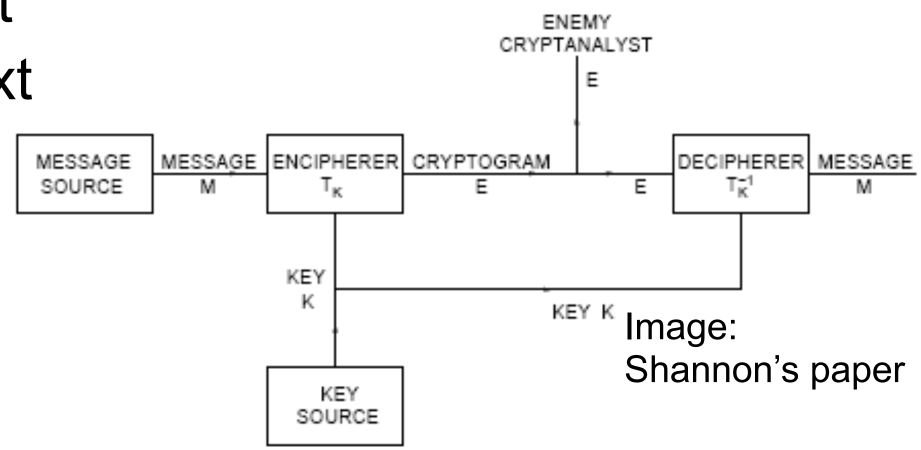


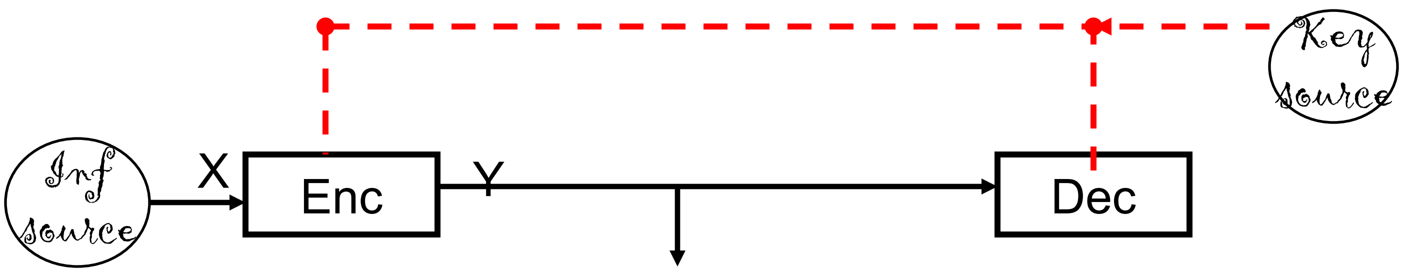
Image:
Shannon’s paper

- Example: Ceasar cipher:
- {a,b,c…z} → {0,1,..25}

- Key = 3
- Enc(k, message) = 3 + message (mod 26)
- Dec(k, ciphertext) = ciphertext - 3 (mod 26)

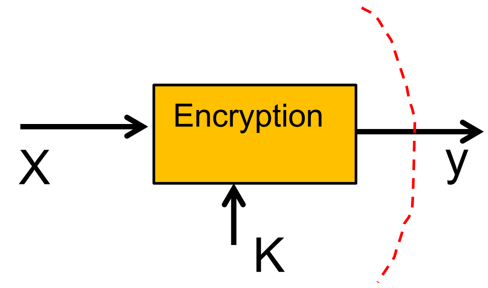
Secrecy systems
Shannon 1949

- A cryptosystem is defined by a 5 tuple $(\mathcal{X},\mathcal{Y},\mathcal{K},\mathrm{Enc},\mathrm{Dec})$
  - $\mathcal{X},\mathcal{Y},\mathcal{K}$ are sets of plaintext, ciphertext and keys, respectively.
  - Enc,Dec are algorithms for encryption and decryption



Reference: Cryptography, Theory and Practice, Douglas Stinson

Secrecy systems

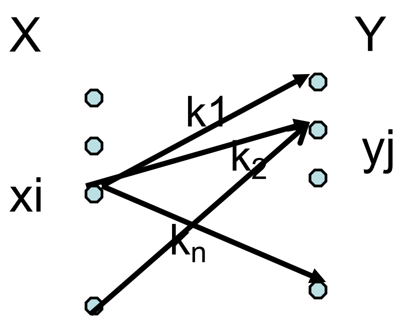


Passive adversary
 Eavesdropping the communication

Eve knows:

- X and p(X)
- K and distribution on K, p(K) (chosen by Alice/Bob)

- Enc (K, X) =Y
- Dec (K, Y)= X



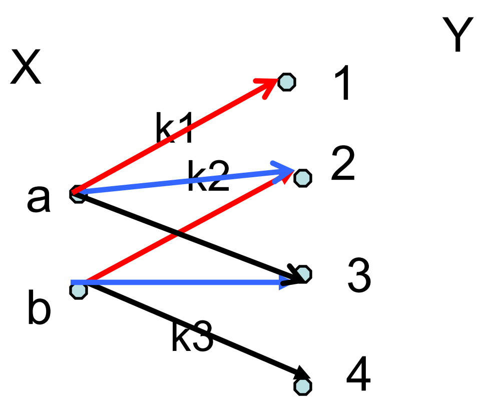
- Using these can calculate p(Y)
- p(X), p(K) ➔ $p(y_j)$ for all y_j

$$p(y_j) = \sum_{x_i} \sum_{\{k_t : Enc(k_t, x_i) = y_j\}} p(k_t)\, p(x_i)$$

Example

- $\mathcal{X}$ ={a,b}, p(X=a) =1/4, p(X=b) = 3/4
- $\mathcal{K}$ ={1,2,3} p(K=1) =1/2, p(K=2) = p(K=3) = 1/4
- $\mathcal{Y}$ ={1,2,3,4}

- p(Y =1) = p(X = a) x p(K =1) =1/4 x1/2 = 1/8
- p(Y = 2) = 1/16+3/8 = 7/16
- p(Y = 3) = 1/4
- p(Y = 4) = 3/16

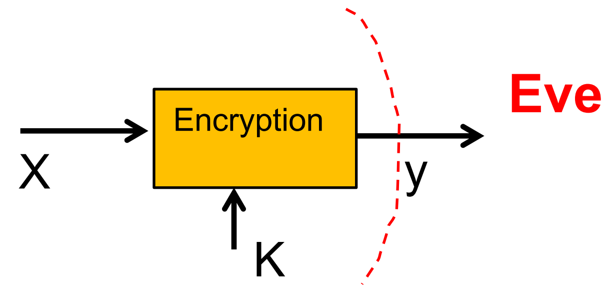


K \ X	a	b
k_1	1	2
k_2	2	3
k_3	3	4

Breaking the cipher

Publicly known:

- The algorithms
- X, K : message and key spaces



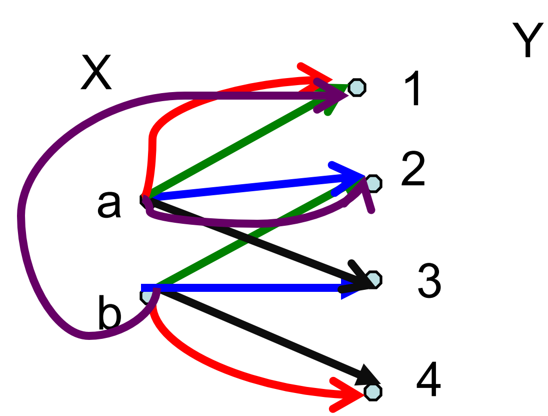
- p (X),p(K): A priori probability distributions

➔Eve can calculate distribution on Y

“Breaking” a cipher

- Eve sees a ciphertext y (e.g. y=2)
- Finding x
- Finding k

- Which goal is less demanding?
  - Achieving it, implies the other.



Perfect Security

- An encryption system ($\mathcal{X}, \mathcal{Y}, \mathcal{K}$, Enc, Dec) is perfectly secure if for any probability distributions on X, we have

$$p(X|y) = p(X)$$

- That is for any message x, any ciphertext y satisfying $p(Y=y)>0$,

$$p(x|y)=p(x), \text{ for all } x,y$$

  - observing y has not changed the original probability of x

➔ Distribution of messages and ciphertexts are independent

  - $p(x,y) = p(x)p(y)$