Recall: 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

➔ Joint distribution of message and ciphertext is,

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

Perfect secrecy

- Lemma: an encryption system $(\mathcal{X}, \mathcal{Y}, \mathcal{K}$, Enc, Dec) is perfectly secure if for all probability distributions p(X), and for any x satisfying p(X=x)>0, and for all y:

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

- Proof:

$$p(Y = y \mid X = x) = \frac{p(Y = y, X = x)}{p(X = x)}$$

$$= p(X = x \mid Y = y) \frac{p(Y = y)}{p(X = x)}$$

- According to definition of perfect secrecy p(X|y) = p(X)

Alternative definition

Lemma:

An encryption system provides perfect security if and only if for,

- Any two messages x_0 and x_1 with non-zero probability and,
- For all ciphertexts y

we have,

$$p(Y = y|X = x_0) = p(Y = y|X = x_1)$$

Proof

1. If perfect secrecy, then $p(y|x) = p(y)$ for all x,y

   ➔ $p(Y=y|X=x_0)=p(Y=y) = p(Y=y|X=x_1)$

2. Conversely, let $p(Y=y|X=x_0)= p(Y=y|X=x_1) = \alpha$. Then,

p(Y=y) **=** $\Sigma_{xi}\, p(Y=y,X=x_i)$ *;marginal dist.*

= $\Sigma_{xi}\, p(X=x_i)\, p(Y=y|X=x_i)$

$= \alpha\, \Sigma_{xi}\, p(X=x_i) = \alpha$ *;prob sum to 1*

- That is $p(Y=y|X=x_0)= \alpha= p(Y=y)$ ➔ *perfect secrecy*

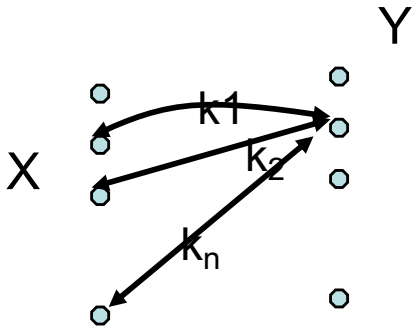
Number of keys

Theorem: In a cryptosystem with perfect secrecy,

A. number of keys is at least the same as the number of messages

B. If $|\mathcal{X}|=|\mathcal{Y}|=|\mathcal{K}|$, then
   - Every key is used with equal probability
   - For every x in $\mathcal{X}$, and every y in $\mathcal{Y}$, there is a unique key k such that Enc(k,x)=y

- Proof: First, show:
  A. Perfect secrecy requires number of keys be at least the same as the number of messages



- For any arbitrary ciphertext y:
- We have $p(x_1|y)= p(x_1)$ for any x_1 with $p(x_1)>0$,
- Then at least one key should map x_1 to y.

- (two messages cannot be mapped to the ciphertext under the same key)

Distribution of keys

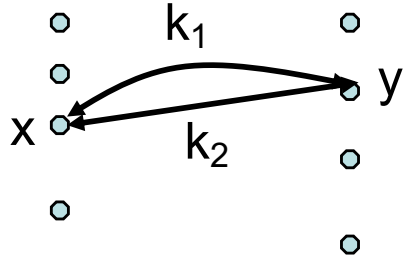
B. If $|\mathcal{X}|=|\mathcal{Y}|=|\mathcal{K}|$ then for every x in $\mathcal{X}$, and every y in $\mathcal{Y}$, there is a unique key k such that Enc(k,x)=y

- *Proof*: Assume that for x in $\mathcal{X}$, with p(X=x)>0 and for a y in $\mathcal{Y}$, we have $Enc(x,k_1)= Enc(x,k_2)=y$

→ ∃ at least one y' such that for any key k_i in $\mathcal{K}$
we have $Enc(x,k_i) \neq y'$

- Thus,

$$p(X=x|Y=y') = 0$$



while p(X=x)>0 → no perfect secrecy

Hence the contradiction!

Distribution of keys

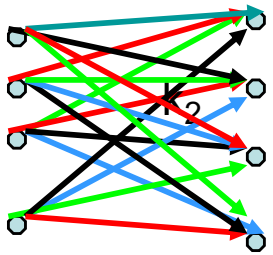
B. If $|\mathcal{X}|=|\mathcal{Y}|=|\mathcal{K}|$ then the keys are uniformly distributed:

- for each x in $\mathcal{X}$, and y in $\mathcal{Y}$, there is exactly one key
Let $|\mathcal{K}|=n$, $\mathcal{X}=\{x_1, x_2,.. x_n\}$, and fix a ciphertext y

$$\Pr(x_i \mid y) = \frac{\Pr(y \mid x_i)\Pr(x_i)}{\Pr(y)}$$

$$= \frac{\Pr(K = k_i)\Pr(x_i)}{\Pr(y)}$$

k_i is such that $Enc(x_i,k_i)=y$



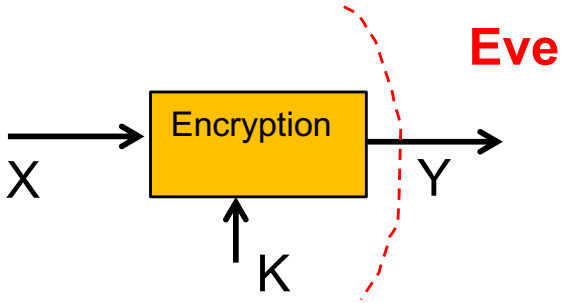
$$For\ perfect\ secrecy\ we\ have\ \Pr(x_i \mid y) = \Pr(x_i)$$

$$\Rightarrow \Pr(k_i) = \Pr(y)\ for\quad 1 \le i \le n$$

$$\text{All keys are used with the same } \Pr(k_i) = \Pr(y)$$

Defining Perfect Secrecy

1. $p(x|y)=p(x)$, for all x,y
   - Equivalently $p(y|x)=p(y)$ for all x,y



2. $H(X|Y)= H(X)$
   - $I(X;Y)=0$

3. $p(y|x_0) = p(y|x_1)$ for all x_0, x_1 ,y

- Definitions 1,2,3, are equivalent.

A system with perfect secrecy:

One time pad

- Vernam 1917

- X, K and Y are binary strings
- For each message bit x, a fresh random key bit is used.

$$Enc(k,x) = k_i \oplus x_i = y_i, \qquad i = 1, \cdots n$$

$$Dec(k,y) = k_i \oplus y_i, \qquad i = 1, \cdots n$$

- We proved for a single bit message, the system provides perfect secrecy.

Enc(x,k): y= x+k mod 2
Dec(y,k): x= y+k mod 2

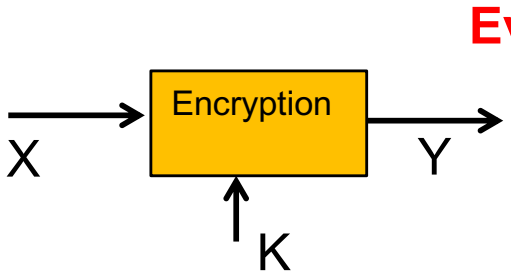
K \ X	0	1
0	1	0
1	0	1

Drawbacks of OTP

- Long keys: length of the key is the same as plaintext
  - One-time-pad will loose perfect security if keys are used twice.

- Requires perfect random keys

Guessing the plaintext



Assume $\mathcal{X}$={a,b} and P(X)=(1/4,3/4)

What is the best guess at plaintext, initially?

Assuming perfect secrecy what is the best guess for plaintext, given a ciphertext?

Y=1 is seen:

→ Guess(Y=1) =b

Y=2 is seen

→ Guess(Y=2) =b

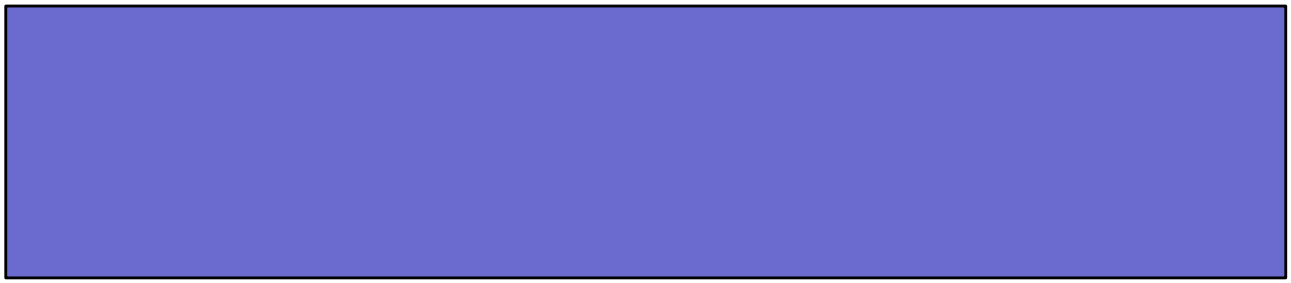
And so on ….

Guessing the plaintext

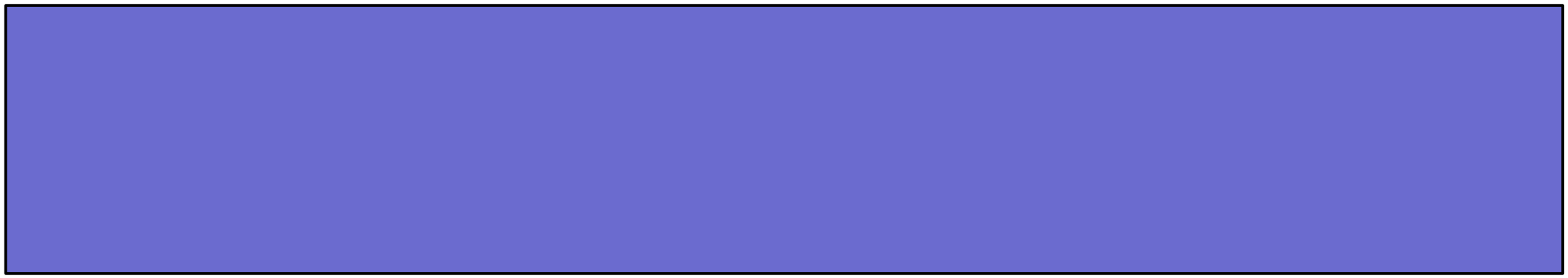
What is the best guess for plaintext, given a ciphertext?

		1/4	3/4
	X / K	a	b
1/2	1	1	2
1/4	2	2	3
1/4	3	3	4

Y=1 is seen:



Y=2 is seen:



Posterior probabilities are used for the best guess.

Cont.

Y=3 is seen:

- Pr (x=a|Y=3) = Pr(Y=3, X=a)/Pr(Y=3) = (1/12)(1/3)=1/4
- Pr (x=b|Y=3) = Pr(Y=3, X=b)/Pr(Y=3) = (1/4)/(1/3) =3/4

→ Guess(Y=3) =b

Y=4 is seen:

- Pr (x=a|Y=4) = Pr(Y=4, X=a)/Pr(Y=4) =0
- Pr (x=b|Y=4) = Pr(Y=4, X=b)/Pr(Y=4) = (3/16)/(3/16) = 1

→ Guess(Y=4) =b

Guessing the plaintext

Assume y_j is given (we have observed y_j)

We want to find the '*best*' guess for x_i

'best' means the probability of being wrong is the smallest.

$$\Pr(x_i \mid y_j) = \frac{\Pr(y_j \mid x_i)\Pr(x_i)}{\Pr(y_j)}$$ Posterior probability

$\Pr(y_j)$ is a normalizing factor- need not be computed when making decision based on y_j

Today's encryption systems

"How can we ever be sure that a system which is not ideal and therefore has a unique solution for sufficiently large N will require a large amount of work to break with every method of analysis? There are two approaches to this problem; (1) We can study the possible methods of solution available to the cryptanalyst and attempt to describe them in sufficiently general terms to cover any methods he might use. We then construct our system to resist this "general" method of solution. (2) We may construct our cipher in such a way that breaking it is equivalent to (or requires at some point in the process) the solution of some problem known to be laborious."

C.E. Shannon (1949)
Communication Theory of Secrecy Systems

DES
(Data Encryption Standard-1977)

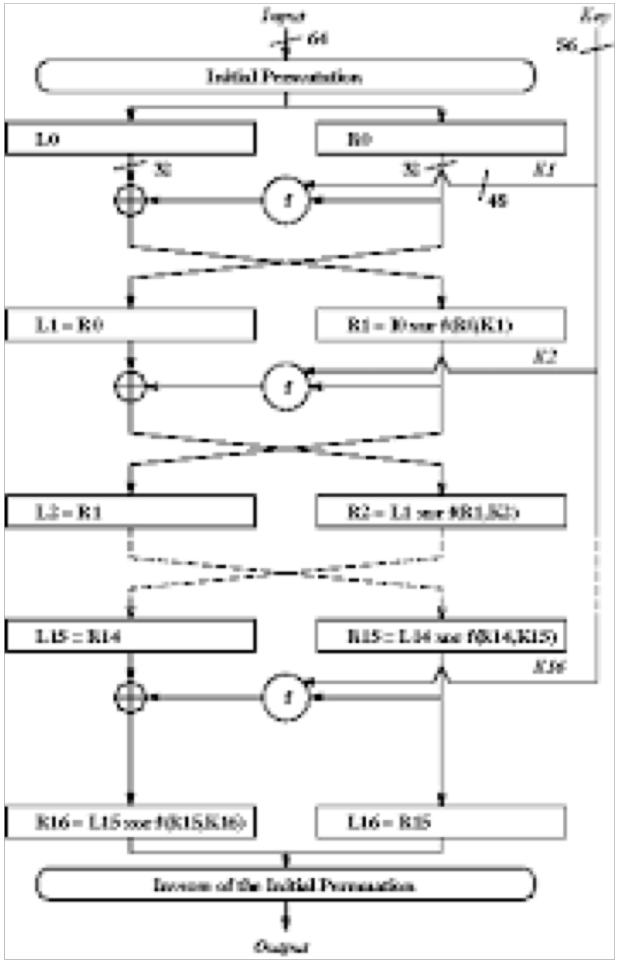
- Messages: 64 bit blocks
- Key: 56 bit

- Encryption can be described as:
  a table with, 2^{56} rows, and 2^{64} columns

- Cannot provide perfect security even for a single block. (Why?)

Today's encryption systems

- Provide security with a short key
  - Randomly chosen
- Use complex functions c= Enc(k,m) that mix the plaintext and the key
  - Each bit of ciphertext depends on plaintext and the key
- How do we evaluate these algorithms?
- Shannon proposed to make encryption systems that *will require a large amount of work to break.*
- He also proposed *"confusion" and "diffusion" principles for designing strong ciphers.*
  - Ciphers that cannot be easily cryptanalized.
  - DES and many modern ciphers use these principles



Data Encryption Standard (DES)

Modern ciphers

- AES (Advance Encryption Standard)

- plaintext alphabet: blocks of 128 bits
- ciphertext alphabet: blocks of 128 bits

- Keys: 128 bits→ 2^{128} Keys

- Security: amount of work for the best attack
  - A substitution table with 2^{128} rows and columns
  - Trying one key each microsecond:

10^{38} microsecond ~ 3 x 10^{24} years