Plan

- Perfect secrecy
  - Alternative definitions
  - Number of keys
- Modern ciphers

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

Security

- For our example:

$$p(a \mid Y=2) = \frac{p(X=a, Y=2)}{p(Y=2)} = \frac{p(X=a)\, p(Y=2 \mid X=a)}{p(Y=2)}$$

$$= p(X=a) \frac{p(Y=2 \mid X=a)}{p(Y=2)}$$

$$= p(X=a) \frac{1/4}{7/16} = p(X=a) \frac{4}{7} = \frac{1}{4} \times \frac{4}{7} = \frac{1}{7}$$

$$\Rightarrow p(X=a) \neq p(X=a \mid Y=2) \Rightarrow \textit{No perfect secrecy}$$

Perfect Secrecy Systems: Example

- Which one may provide perfect secrecy:

X / K	0	1
k_1	0	0
k_2	1	0

X / K	0	1
k_1	1	0
k_2	0	1

X / K	0	1
1	1	0
0	0	1

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

Perfect Secrecy Systems: Example

- Does the system provides perfect secrecy for,
- Key dist : $p(K=0) = p(K=1) = 1/2$
- Message dist: $p(X=0) = 1/3$ $p(X=1)=2/3$

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

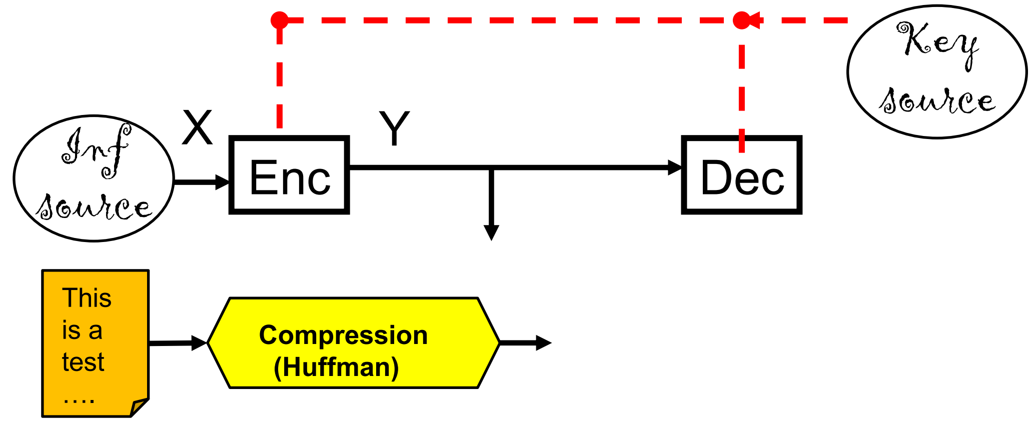
- Perfect secrecy
- $p(X=0|Y=0) = p(X=0,Y=0)/p(Y=0)$
- $p(X=0,Y=0) = p(X=0)p(Y=0|X=0) = (1/3)(1/2)$
- $p(Y=0) = p(K=0).p(X=1) + p(K=1).p(X=0) = 1/2$

- $p(X=0|Y=0)= (1/3)(1/2)/(1/2) =1/3 =p(X=0)$
- $p(X=1|Y=0)= (2/3)(1/2)/(1/2) =2/3 = p(X=1)$
- ..

- The system provides perfect secrecy for the source.

Perfect Secrecy Systems: Example

- Multiple source output:
- X is a binary DMS:
  - uniform distribution
  - $p(X=0) = p(X=1) = 1/2$
  - $H(X) = 1$ bit/symbol
- Key: $p(K=0)=p(K=1)=1/2$



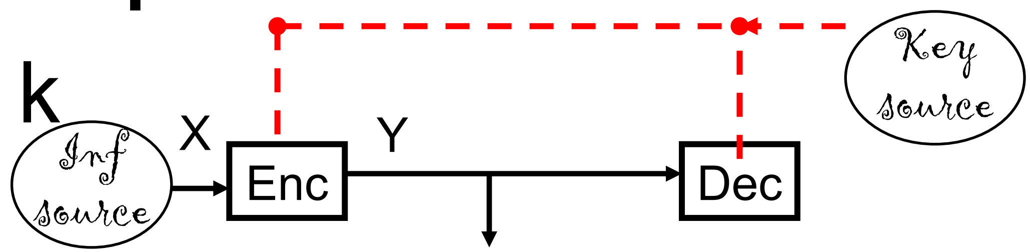
- Entropy of a sequence of 3 message symbols:
- $H(X_1X_2X_3)= H(x_1)+H(X_2)+H(X_2) = 3$ bits

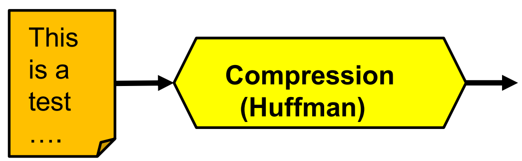
K \ X	0	1
1	1	0
0	0	1

Perfect Secrecy Systems: Examples

- Alice and Bob use k
- Eve sees $y_1y_2y_3$
- $y_1= k + x_1$
- $y_2= k + x_2$
- $y_3= k + x_3$

- $\rightarrow y_1+y$= x +x
- $\rightarrow y_1+$





- Perfect secercy for a single bit
- New key for each symbol

K \ X	0	1
1	1	0
0	0	1

Vigenère Cipher

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O		
19	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N				
19	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N					
20	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O					
21	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P					
22	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q					
23	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R					
24	Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S					
25	Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T					

Named after
Blaise de Vigenère

Invented first by
Giovani Battista Bellas
1553

- Each row is a shift cipher.
- Enc(x,k): $y = x+k \mod 26$
- Dec(y,k): $x = y-k \mod 26$

Vigenère Cipher

- Perfect secrecy?
- $p(X=a) = p_a$
- $p(X=a|\ Y= t) = p(X=a) = p_a$
- (Verify)

- Perfect secrecy for single letter

Vigenère Cipher

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Key period= 5

Plaintext:
ATTACKATDAWN

Key:
LEMONLEMONLE

Ciphertext:
LXFOPVEFRNHR

No perfect secrecy if the key is not randomly generated for each plaintext symbol.

Perfect secrecy

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

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

- Proof:

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

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