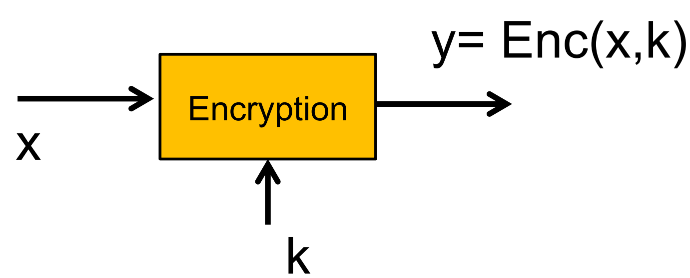
- Assignment 2 deadline
  ** Friday Oct 26, 11:59 pm**

- Midterm on Tuesday, Oct 30

Perfect Secrecy

1. $p(x|y)=p(x)$, for all x,y
2. $p(y|x) =p(y)$, for all x,y
3. $p(y|x_0) = p(y|x_1)$, for all y and any x_0, x_1
4. $H(X|Y)= H(X)$
5. $I(X;Y)=0$
6. $|\mathcal{K}| \geq |\mathcal{X}|$
7. If $|\mathcal{X}|=|\mathcal{Y}|=|\mathcal{K}|$, then
   A. K~Unif($|\mathcal{K}|$)
   B. For any x,y, there is a unique k s.t. Enc(x,k)=y



Systems without Perfect Secrecy

- Seeing a ciphertext "leaks information" about the plaintext.

→ Can we allow "small amount of leakage" but have a shorter key?

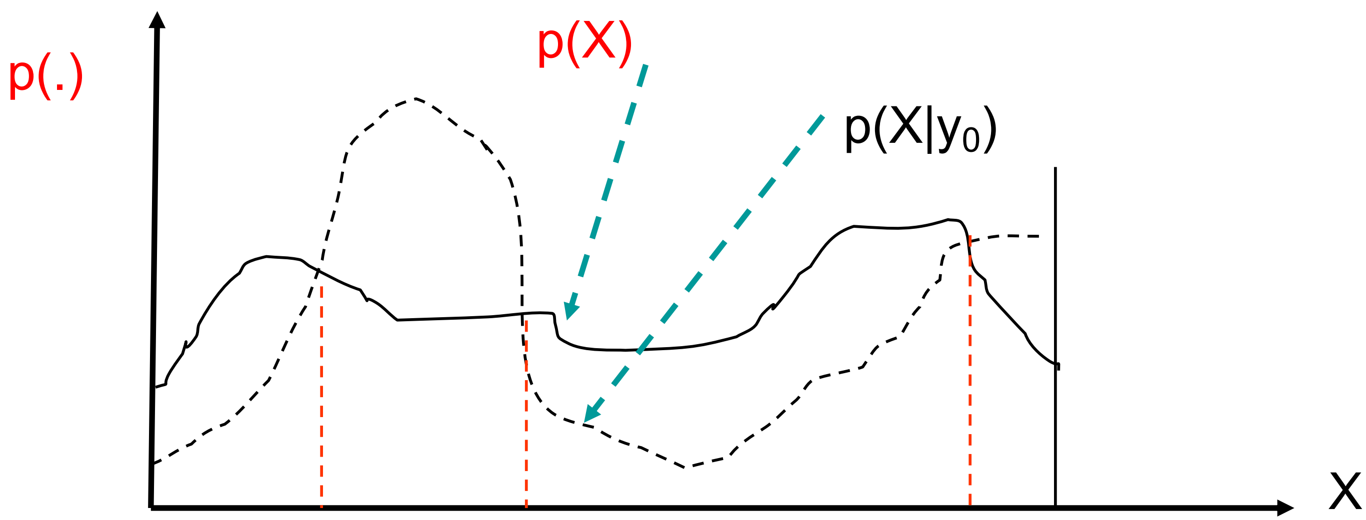
*** First we need to measure "leakage"**

- Measuring leakage
  - Improved probability of guessing the plaintext after the "leakage"
  - Reduced entropy after the "leakage"

Defining ε-secrecy

- We want to say,

"observing y has changed the distribution of plaintext space by ε"

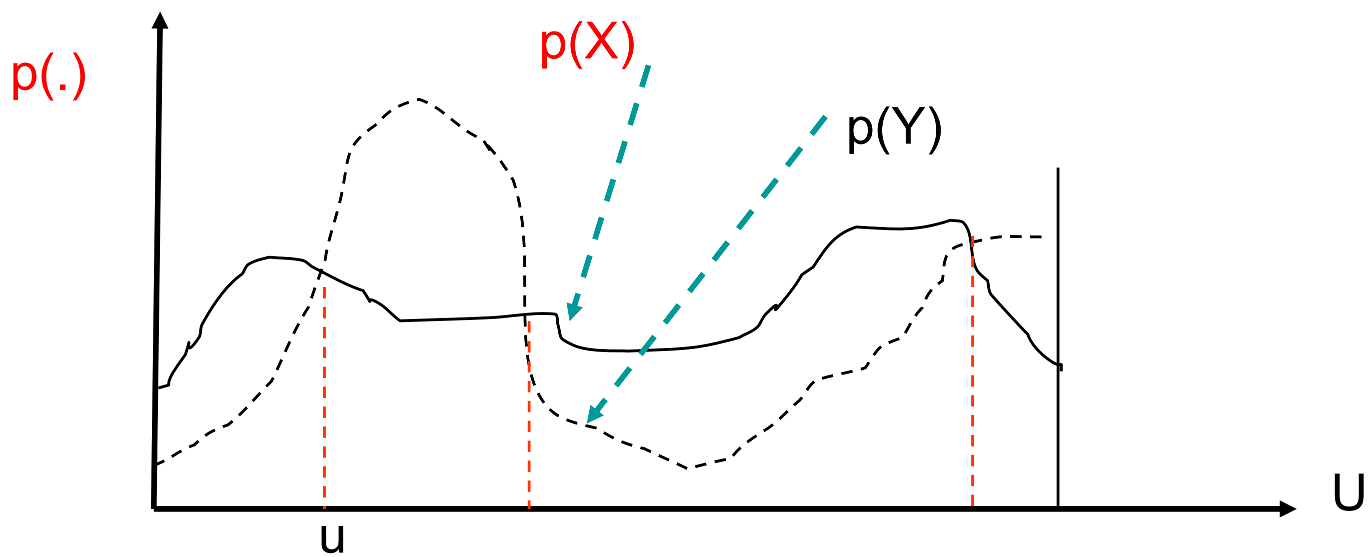


Distance between distributions

Statistical distance

$$SD(X,Y) = SD(P_X, P_Y) := \frac{1}{2}\sum_{u \in U} | P_X(u) - P_Y(u) | \leq \varepsilon$$

Defined for the whole distribution

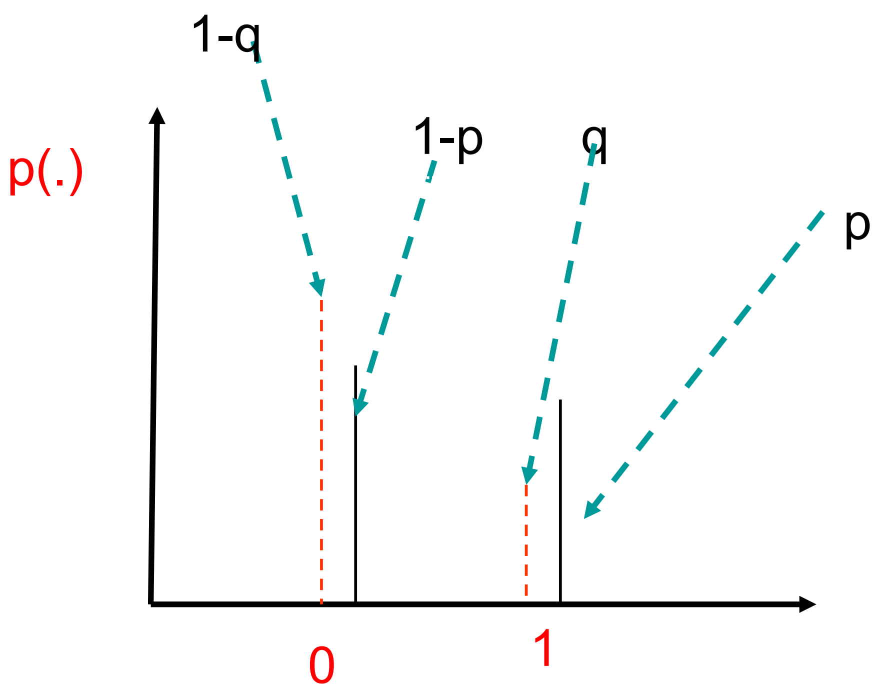


Example

- Statistical distance between two biased coins

$$SD(P_X, P_Y) = \frac{1}{2}[|p-q| + |1-p-(1-q)|]$$

$$= |p-q|$$



Defining ε-secrecy

Use statistical distance between distributions to bound the information leakage when observing each ciphertext:

For all y_j, $SD(\ p(X)\ ,\ p(X|y_j)\ ) < \varepsilon$

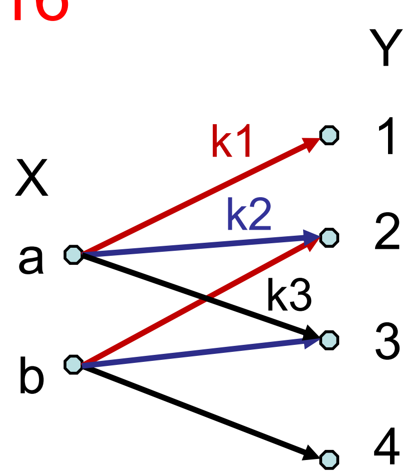
Upper bound on leackage

Recall the 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) × p(K =1) =1/4 × 1/2 = 1/8
- p(Y = 2) = 1/16+3/8 = 7/16
- p(Y = 3) = 1/4
- p(Y = 4) = 3/16



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

How much secrecy?

Perfect secrecy

- For all ptxt, ctxt pairs: p(a|1) = p(a), p(a|2)=p(a)..
- For any pair of ptxts, here only {a,b}, and any ctxt, p(1|a)=p(1|b)…

ε-security

- Possible definitions:
  1. For all y, H(X) -H(X|y) <ε
  2. For all y, SD(p(X) , p(X|y)) < ε

     …..

Do you know any other measure?

$$p(X=a\,|\,Y=1)=\frac{p(X=a)p(Y=1\,|\,X=a)}{p(Y=1)}=\frac{(1/4)\times(1/2)}{1/8}=1$$

$$p(X=b\,|\,Y=1)=\frac{p(X=b)p(Y=1\,|\,X=b)}{p(Y=1)}=\frac{(3/4)\times 0}{1/8}=0$$

$$p(X=a\,|\,Y=2)=\frac{p(X=a)p(Y=2\,|\,X=a)}{p(Y=2)}=\frac{(1/4)\times(1/2)}{7/16}=1/7$$

$$p(X=b\,|\,Y=2)=\frac{p(X=b)p(Y=2\,|\,X=b)}{p(Y=2)}=\frac{(3/4)\times 1/2}{7/16}=6/7$$

$$p(X=a\,|\,Y=3)=\frac{p(X=a)p(Y=3\,|\,X=a)}{p(Y=3)}=\frac{(1/4)\times(1/4)}{1/4}=1/4$$

$$p(X=b\,|\,Y=3)=\frac{p(X=b)p(Y=3\,|\,X=b)}{p(Y=3)}=\frac{(3/4)\times 1/4}{1/4}=3/4$$

$$p(X=a\,|\,Y=4)=\frac{p(X=a)p(Y=4\,|\,X=a)}{p(Y=4)}=\frac{(1/4)\times 0}{3/16}=0$$

$$p(X=b\,|\,Y=4)=\frac{p(X=b)p(Y=4\,|\,X=b)}{p(Y=4)}=\frac{(3/4)\times 1/4}{3/16}=1$$

$$p(x \mid y) \neq p(x)$$

$$p(X = a \mid Y = 1) = 1 \neq 1/4 = p(X = a) \quad \Rightarrow \text{No perfect secrecy}$$

$$(1/2) \mid p(X = a \mid Y = 1) - p(X = a) \mid + \mid p(X = b \mid Y = 1) - p(X = b) \mid =$$

$$(1/2) \mid 1 - 1/4 \mid + \mid 0 - 3/4 \mid = 3/4$$

$$(1/2) \mid p(X = a \mid Y = 2) - p(X = a) \mid + \mid p(X = b \mid Y = 2) - p(X = b) \mid =$$

$$(1/2) \mid 1/7 - 1/4 \mid + \mid 6/7 - 3/4 \mid = 3/28$$

$$(1/2) \mid p(X = a \mid Y = 3) - p(X = a) \mid + \mid p(X = b \mid Y = 3) - p(X = b) \mid =$$

$$(1/2) \mid 1/4 - 1/4 \mid + \mid 3/4 - 3/4 \mid = 0$$

$$(1/2) \mid p(X = a \mid Y = 4) - p(X = a) \mid + \mid p(X = b \mid Y = 4) - p(X = b) \mid =$$

$$(1/2) \mid 0 - 1/4 \mid + \mid 1 - 3/4 \mid = 1/4$$

Measuring leakage in "bits": ε-secrecy

- How much information observation Y=y contains about plaintext X.

- Reduction in uncertainty of plaintext after observing a ciphertext y:

$$H(X) - H(X|Y=y)$$

- $H(X) - H(X|y_j) < \varepsilon_j$ for all y_j

$$\varepsilon = \max_j \varepsilon_j$$

Defining ε-secrecy

- p(X) uniform
- p(K) uniform
- H(X)=log 3~ 1.5 bit

- H(X) - H(X|Y=1) = 0.5 bit
- H(X) - H(X|Y=2) = 0.5 bit
- H(X) - H(X|Y=3) = 1.5 bit
- ε=1.5 bit
- Y=3 is completely insecure

- H(X|Y) = 0.65 bit
- H(X)- H(X|Y) ~ 0.9 bit

	$X=1$	$X=2$	$X=3$
$k=1$	1	3	2
$k=2$	2	3	1

$$p(X=1)=p(X=2)=p(X=3)=\frac{1}{3}$$

$$p(k=1)=p(k=2)=\frac{1}{2}$$

$$p(Y=1)=p(Y=2)=p(X=3)=\frac{1}{3}$$

$$H(X\mid Y=1)$$

$$H(X\mid Y=3)$$

$$H(X\mid Y)=$$

$$H(X)=1.5 \quad bits$$

Key length

- It can be proved that allowing small leakage does not substantially reduce the key length.

- Roughly,
- $I(K;M) < \varepsilon \quad \rightarrow H(K) > H(M) - \varepsilon$

How much secrecy?

Perfect secrecy

- For all ptxt, ctxt pairs: p(1|a) = p(1)….
- For any x_0,x_1 (only {a,b}), and any ctxt, p(1|a)=p(1|b)…

ε-security

- |H(X|y)-H(X)| <ε
- SD(p(X|y), p(X)) <ε
- ……

If you do the calculations and ε=0,

- Game based definition

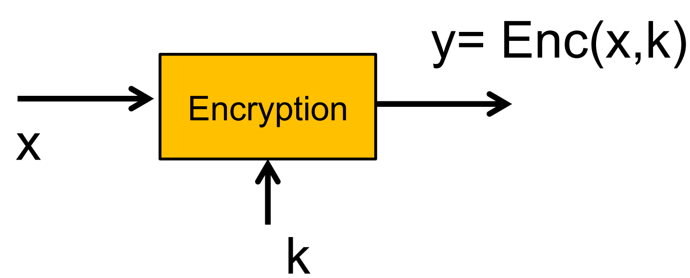
Summary

- Secrecy scenario – eavesdropping adversary

- Perfect secrecy
  - Equivalent definitions
  - Number of keys

Perfect Secrecy (Summary)

1. $p(x|y)=p(x)$, for all x,y
2. $p(y|x) = p(y)$, for all x,y
3. $p(y|x_0) = p(y|x_1)$, for all y and any x_0, x_1
4. $H(X|Y)= H(X)$
5. $I(X;Y)=0$
6. $|\mathcal{K}| \geq |\mathcal{X}|$
7. If $|\mathcal{X}|=|\mathcal{Y}|=|\mathcal{K}|$, then
   A. $K \sim \mathrm{Unif}(|\mathcal{K}|)$
   B. For any x,y, there is a unique k s.t. Enc(x,k)=y



Summary

- Secrecy scenario – eavesdropping adversary

- Perfect secrecy
  - Equivalent definitions
  - Number of keys

- ε-secrecy
  - Entropy based
  - Statistical distance

  …

  ε means different for each measure