Cryptography & Complexity

$k \in_R \{0,1\}^n \longleftarrow$ Private key (uniform random string)

Alice $\Longrightarrow$ Bob

$x \in_R \{0,1\}^m \quad y = E_k(x) \quad x = D_k(y)$

$\uparrow$

Eve

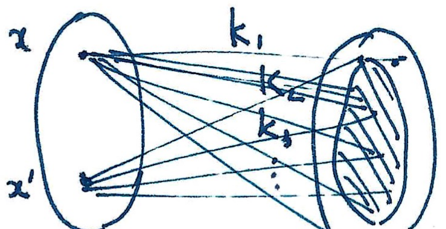
knows y, n, m

<u>Decryption works</u>: $\forall\, k, x \quad D_k(E_k(x)) = x$

$\forall\, x, x' \in \{0,1\}^m \;\forall\, k \quad E_k(x) \neq E_k(x')$

<u>Def (Perfect ~~secrecy~~ secrecy)</u>: (E, D) is an encryption scheme.

(E,D) is <u>perfectly secret</u> if $\forall\, x, x' \in \{0,1\}^m \;\forall\, k$, the distributions of $E_k(x)$ and $E_k(x')$ are identical ($k \in_R \{0,1\}^m$).



Plaintext x Ciphertext y

(Implicitly assume Eve is computationally all powerful.)

<u>One time pad [Shannon]</u>: $n = m \quad E_k(x) = x \oplus k$ (bitwise XOR)

Achieves Perfect Secrecy. $\quad D_k(y) = y \oplus k$

Can be used only once! $\quad (x \oplus k) \oplus (x' \oplus k) = x \oplus x'$

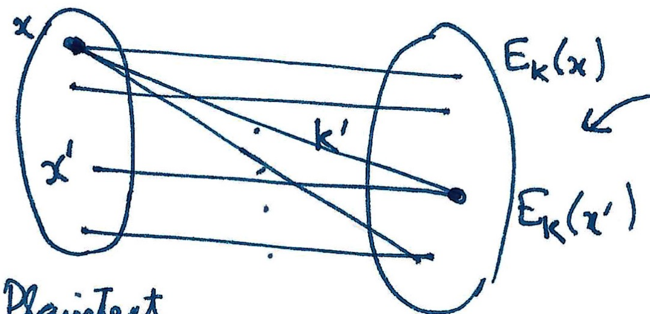
Clm: No perfectly secret encryption scheme can have key length shorter than message length

$$\left(\text{Perfect secrecy} \Rightarrow \underbrace{n}_{\text{key length}} \geq \underbrace{m}_{\text{Message length}}\right)$$

One-time pad, $n = m$, hence optimal

Proof:

Fix a choice of $k \in \{0,1\}^n$



Plaintext Message $x \in \{0,1\}^m$

Ciphertext Encryption $E_K(x)$

How many possible ciphertexts? 2^m

For a fixed key, there are 2^m ciphertexts.

For every $x' \in \{0,1\}^m$, there exists a key k' s.t.

$$E_{K'}(x) = E_K(x')$$

(Perfect secrecy, x must have some chance of mapping to $E_K(x')$.)

Thus, $E_{K'}(x)$ (fixed x, varying k') must take on at least 2^m values. Hence, there are at least 2^m distinct keys, so $n \geq m$. ∎

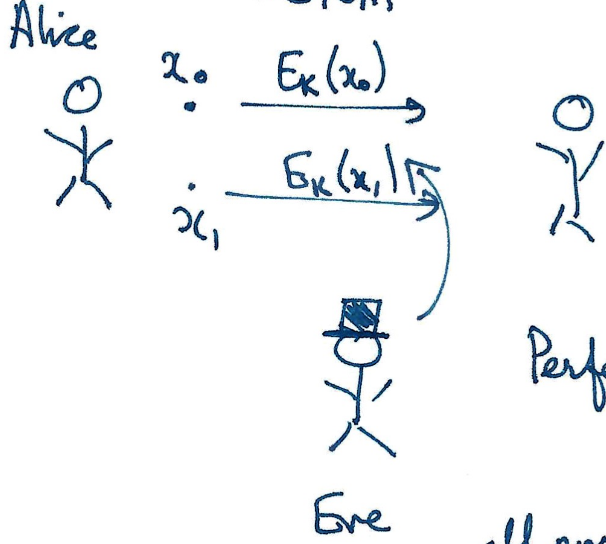
Let's assume Eve is computationally bounded
(Eve runs in polynomial time.
Eve runs the "breaking" function B)

Eve runs $B(y)$ and wants to infer something about x. $(\cancel{x}\ y = E_K(x))$

$\boxed{\text{and } n < m.}$

Lemma: Suppose $\mathbb{P} = \mathbb{NP}$. Let (E, D) be an encryption scheme running in polytime. Then $\exists$ poly time B s.t $\forall m$, there exist two messages that B can distinguish

$$\left(\exists\, x_0, x_1 \text{ s.t. } \Pr_{\substack{k \in_R \{0,1\}^m \\ b \in \{0,1\}}} \left[\cancel{B(A}\ B(E_K(x_b)) = b \right] \geq \frac{3}{4}\right)$$

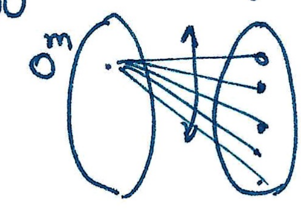


Perfect secrecy: guessing prob $= 1/2$

all possible encryptions of 0^m

Proof: Let $n < m$. Let $S \subseteq \{0,1\}^*$ be the support of $E_K(0^m)$, where $k \in_R \{0,1\}^m$.

All keys



The language S is in $\mathbb{NP}$ (Cert. is k). Hence S is in $\mathbb{P}$.

Consider the following procedure B

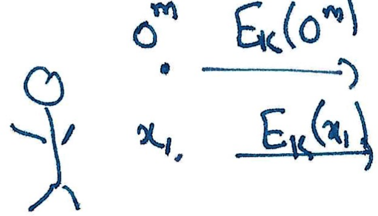
B : on input y

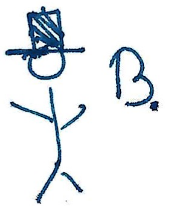
(1) Determine if $y \in S$ (poly time). If so, output 0

(2) Else output 1.

Clm : $\exists$ message x_1 s.t. $\Pr_k [B(x_1) = 1] \geq 1/2$

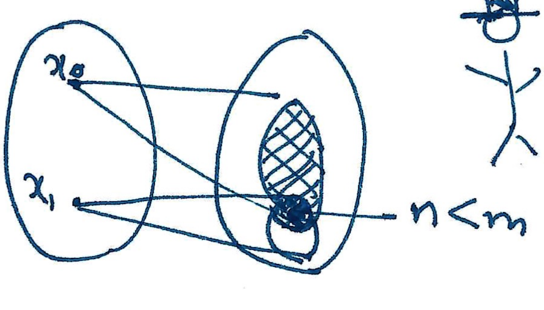
$$\Pr_k [B(x_1) = 1] = \Pr_k [E_k(x_1) \notin S]$$



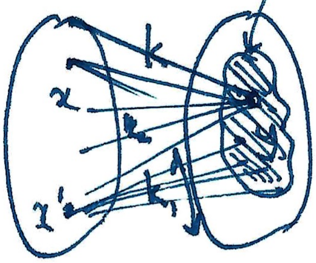


$$\Pr_{\substack{k \\ b \in \{0,1\}}} [B(x_b) = b] = \frac{1}{2} \underbrace{\Pr_k [B(x_0) = 0]}_{1} + \frac{1}{2} \underbrace{\Pr_k [B(x_1) = 1]}_{\geq 1/2}$$

$$\geq \frac{3}{4}.$$



Proof :



$E_k(x) = y$

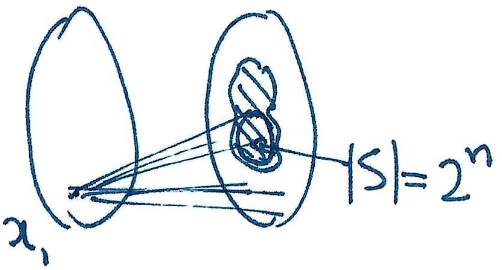
By 1-1 of encryption, there are at most $\overset{\#\text{keys}}{2^n}$ edges into y. ~~Deg(y)~~ Degree of $y \leq 2^n$

$|S| \leq 2^n$ $\quad$ #edges into $S \leq 2^n \times 2^n = 2^{2n}$

For every x, let $d(x)$ be #edges from x into S

$$\sum_{x \in \{0,1\}^m} d(x) \leq 2^{2n} \qquad \text{Avg } d(x) \leq \frac{2^{2n}}{2^m}$$

$$\text{Avg } d(x) \leq \frac{2^{2n}}{2^m} \leq \frac{2^{2n}}{2^{n+1}} = \frac{2^n}{2} \qquad \begin{pmatrix} n < m \\ m \geq n+1 \end{pmatrix}$$



$\exists\, x_1$ s.t. $d(x_1) \leq \frac{2^n}{2}$

Hence $\Pr_k[E_k(x_1) \in S] \leq \frac{1}{2}$

$\Pr_k[E_k(x_1) \notin S] \geq 1/2$ ∎

<u>Def</u>: A function $\varepsilon : \mathbb{N} \to [0,1]$ is negligible if $\varepsilon(n) = n^{-\omega(1)}$ $\left(\varepsilon(n) \leq \frac{1}{n^c} \;\; \forall c \in \mathbb{N}\right)$

A bit with bias $\varepsilon(n)$ is indistinguishable from a (uniform) random bit.

<u>Def</u>: [One-way fn] A polytime computable fn. $f : \{0,1\}^* \to \{0,1\}^*$ is a <u>1-way fn.</u> if $\forall$ polytime procedures B $\exists$ negligible fn. ε.

$$\forall m \quad \Pr_{x \in_R \{0,1\}^m}\Big[B\big(f(x)\big) = x' \text{ and } f(x) = f(x')\Big] \leq \varepsilon(n)$$

<u>Inversion is hard</u>

<u>Conjecture</u>: There exists a 1-way function.

(Multiplication is a 1-way function)

Two prime numbers p, q each n bits long.

$f(p,q) = p \times q$

Inversion problem: given product pq, compute p & q.

Believed that factoring is hard. factoring not poly time

<u>Clm</u>: Existence of 1-way fn $\Rightarrow \mathbb{P} \neq \mathbb{NP}$

<u>Proof</u>: If $\mathbb{P} = \mathbb{NP}$, 1-way fns. do not exist.

B (on input y)

(1) Non-deterministically guess x

(2) Check if $f(x) = y$. If so, output x.

poly time

B is a non-deterministic poly time machine.

If $\mathbb{P} = \mathbb{NP}$, B can be simulated in poly time. And B succeeds w.p. 1 over input. f is not a 1-way fn. ∎

Def [Computationally Secure Encryption]:

(E,D) is an encryption scheme that runs in poly time.

The scheme is computationally secure if $\forall$ poly time (breaking) procedures B and $\forall\ i \leq m$

$$\Pr_{\substack{k \in \{0,1\}^n \\ x \in \{0,1\}^m}} \left[B(E_k(x)) = x_i \right] \leq \frac{1}{2} + \varepsilon(n)$$

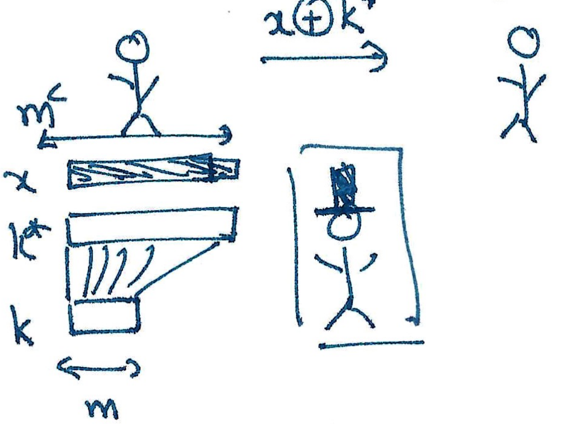
i^{th} bit of message

Thm: Suppose 1-way functions exist. Then $\forall\ c \in \mathbb{N}$ $\exists$ computationally secure encryption scheme where message length $m = n^c$

(Message is polynomially larger than key)

PseudoRandom Generator (PRG)

PRGs are approach to proving above Thm.

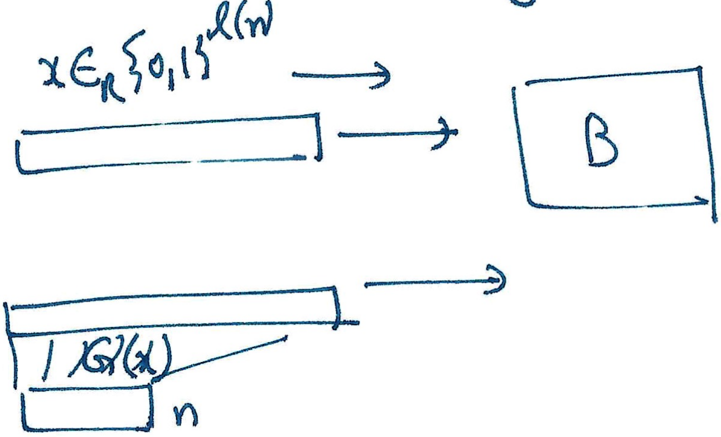


k^* is a "pseudo random" string of longer length

k^* looks random to any poly time machine

<u>Def [PRG]</u>: Let G be a poly time computable fn. and $l : \mathbb{N} \to \mathbb{N}$. G is a secure PRG of stretch $l(n)$ if $\forall x$ $|G(x)| = l(|x|)$ and $\forall$ prob. poly time breaking procedures B $\exists$ negligible fn. $\varepsilon(n)$ s.t.

$$\Big| \underbrace{\Pr_{x \in_R \{0,1\}^{l(n)}} [B(x) = 1]}_{\text{Truly Random}} - \underbrace{\Pr_{x \in_R \{0,1\}^{n}} [B(G(x)) = 1]}_{\text{Pseudo-random}} \Big| \leq \varepsilon(n)$$



<u>Thm</u>: If 1-way fns exist, $\forall c \in \mathbb{N}$ $\exists$ secure PRG of stretch $l(n) = n^c$.