# CSE 599B Lecture 2

Note Title 1/6/2006

alternate view of

Let $M_0, M_1 \in \mathcal{M}$

perfect security $\equiv$ Dist $E_K[M_0]$

$E_K[M_1]$

are the same for $K \xleftarrow{R} \mathcal{K}$

and any two $M_0, M_1$

Any perfectly secure symmetric encryption requires $|\mathcal{M}| \leq |\mathcal{K}|$

Proof: fix any $M$. There are at most $|\mathcal{K}|$ different encryptions of $E_K(M)$ possible of different choices of $K$ in script $\mathcal{K}$

By equivalent def. above

$$S = \{ E_k(M_0)\ k \in \mathcal{K} \} = \{ E_k(M_1) \mid k \in \mathcal{K} \}$$

set of possible ciphertexts

$\therefore$ only $|\mathcal{K}|$ ciphertexts possible

Unique decoding requires at least $|\mathcal{M}|$ possible ciphertexts

# MAC security

$\mathcal{M}$ message space

$\mathcal{T}$ tag space

$\mathcal{K}$ Key space

Tag generation Function

$$T_K(M)$$

$$T: \mathcal{M} \times \mathcal{K} \to \mathcal{T}$$

receiver check

$$T_K(m') = t'$$

## Desirable properties

$\forall M, t \quad Pr_K[T_K(M) = t]$ is small

ideally $\frac{1}{|\mathcal{T}|}$

tags uniformally distributed

$\forall A: \mathcal{M} \times \mathcal{T} \to \mathcal{M} \times \mathcal{T}$ adversary function

$\forall M \in \mathcal{M}$

$Pr_{\mathcal{K}}[A(M, T_K(M)) = (m', t')$ such that

$M' \neq M$ and $T_K(M') = t']$

is small ideally $\frac{1}{|\mathcal{T}|}$

Easily achievable:

Pairwise independent (Universal Hash Functions Families)

ex. $h_{a,b}(m) = am + b \pmod{p}$ where $p$ is prime

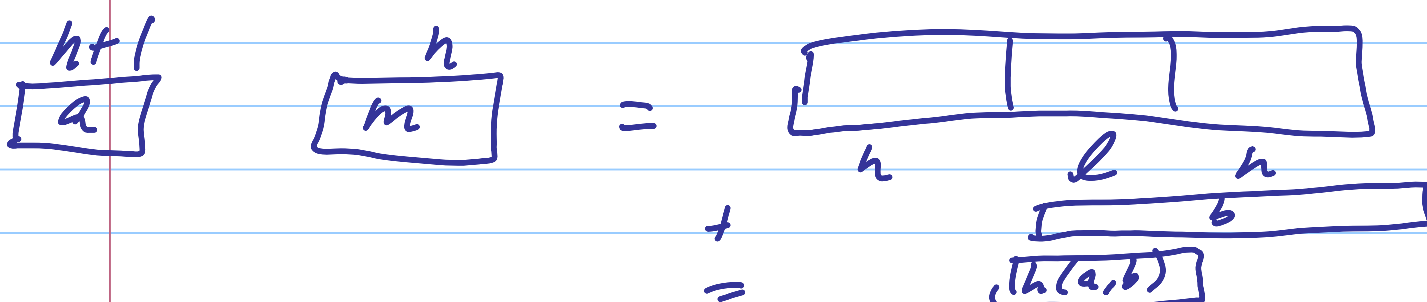
$\mathcal{M} = \mathbb{Z}_p = \mathcal{T}$

$\mathcal{K} = \mathbb{Z}_p \times \mathbb{Z}_p$

$\mathcal{M} = \{0,1\}^n, \quad \mathcal{T} = \{0,1\}^\ell$

$\mathcal{K} = \{\{a,b\} \mid a,b \in \{0,1\}^{n+\ell}\}$

$h_{a,b}(m) =$ middle $\ell$ bits of $am+b$



$am+b=t$ $\quad\quad m \neq m'$

$am'+b=t'$

$$\begin{bmatrix} m & 1 \\ m' & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} t \\ t' \end{bmatrix}$$

$$\Pr_{a,b}\left[h_{a,b}(m)=t\right] = \frac{1}{p}, \quad \Pr_{a,b}\left[h_{a,b}(m)=t, h_{a,b}(m')=t'\right] = \frac{1}{p^2}$$

For $m \neq m'$ $\begin{bmatrix} m & 1 \\ m' & 1 \end{bmatrix}$ is invertible

$\Rightarrow$ exactly one choice of $a,b$ that works

$$\Pr_{a,b}\left[h_{a,b}(m')=t' \mid h_{a,b}(m)=t\right] = \frac{1}{p}$$

For $m'=m$

Cryptanalysis cycle

Keep trying to improve cryptosystems based on attack methods

"provable security under specific assumptions"

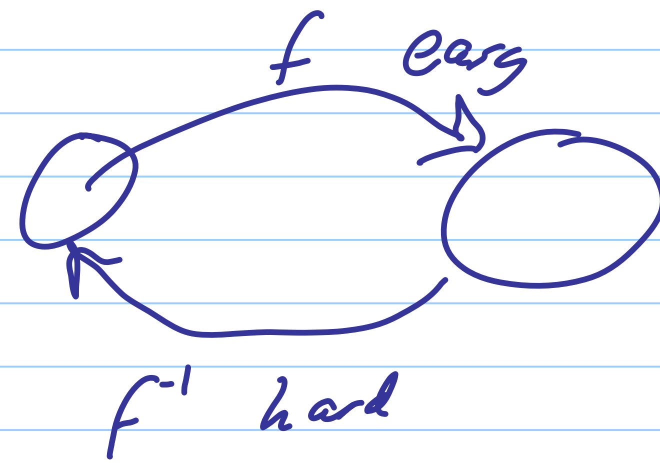
reductions between primitives

One-way functions

pseudorandom functions

$f$ is easy

but $f$ inverse is hard




Symmetric encryption

ex. $f(a,b) = a \times b$ multiplication

$f^{-1}$ factoring

Trapdoor functions

look hard, but with a short secret, you get an easy path.

Security:

assumptions: parties are probabilistic polynomial time

---

definition: A function $\nu : \mathbb{N} \to \mathbb{R}^{\geq 0}$ is negligible iff

$$\nu(n) \text{ is } \frac{1}{n^{\omega(1)}}$$

$\nu(n)$ goes to 0 faster than any polynomial function of $n$

eventually $\nu(n) \leq \frac{1}{n^c}$ for any $c$

Defn: A sequence of probability distributions $\mathcal{D} = \{D_n\}_{n \in \mathbb{N}}$ where $D_n$ is a distribution on $\{0,1\}^n$ is called an ensemble.

Defn: Given two distributions $D_n$ and $\mathcal{E}_n$ on $\{0,1\}^n$

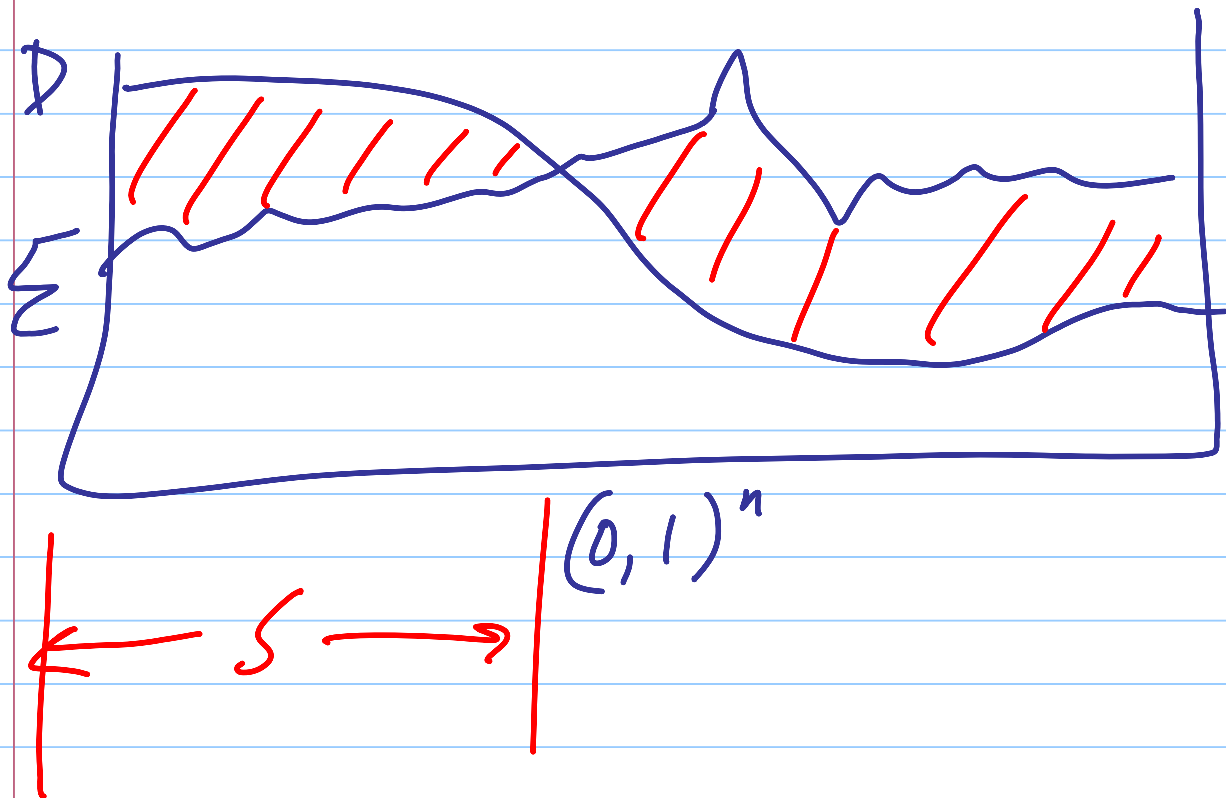
statistical distribution between $D_N$ and $\mathcal{E}_N$

$$\mathrm{dist}(D_N, \mathcal{E}_N) = \frac{1}{2} \sum_{x \in \{0,1\}^n} \left| \Pr_{D_N}[x] - \Pr_{\mathcal{E}_N}[x] \right|$$

$$= \max_{S \subseteq [0,1]} \left( \Pr_{D_N}(S) - \Pr_{\mathcal{E}_N}(S) \right)$$

Defn: Two ensembles $D_N$ and $E_N$ are statistically indistinguishable iff there is a negligible function such that

$$\forall n \quad \text{dist}(D_N, E_N) \le \varepsilon(n)$$




$$\varepsilon(n) = \frac{1}{2^{n/3}}$$

Security parameter $k$

Key distribution algorithm gets $1^k$

$$E_K(M, 1^k)$$

$$D_K(C, 1^k)$$

Key Generation$(1^k)$ produces $K$

previously, $E_K(m_0)$ $E_K(m_1)$ identical distributions

slightly weaker $E_K(m_0)$ $E_K(m_1)$ Statistically close

Statistical distance $\varepsilon(k)$ where $\varepsilon$ is negligible

Similar problems to Shannon's lower bound.

Def$^n$ Two ensembles $\mathcal{D}$ and $\mathcal{E}$ are computationally indistinguishable iff for all probabalistic polynomial time algorithms $A$

$$\varepsilon(n) = \left| \Pr_{x \in \mathcal{D}} [A(x) = 1] - \Pr_{x \in \mathcal{E}} [A(x) = 1] \right|$$

is a negligible function of $n$.

[Yao]

ex. compare $\mathcal{D}$ to $\mathcal{U}$

$\mathcal{D}$ looks random when negligible distance from $\mathcal{D}$ to $\mathcal{U}$ in polynomial time.

next time → systems people use in practice

block ciphers

stream ciphers