Last class:

Equality of distributions

One-time security: $\forall$ m, m' in $\mathcal{M}$: $Enc(K,m) \equiv Enc(K,m')$

where K is random in $\mathcal{K}$

One-Time Pad: $Enc(k,m)=k \oplus m$

perfect security!

Today:

Many-time security

Pseudo-random functions

Construction

AES (Advanced Encryption Standard)

Definition:

Indistinguishabilty against Chosen plaintext attacks

(Ind CPA, or CPA for short):

An encryption scheme (Enc, Dec) is CPA secure if for any

$m_1, m_2, \ldots, m_t$ in $\mathcal{M}$ and $m'_1, m'_2, \ldots, m'_t$ in $\mathcal{M}$

$$(Enc(k,m_1),\ldots Enc(k,m_t)) \overset{\approx}{\uparrow} (Enc(k,m'_1),\ldots,Enc(k,m'_t))$$

computational
indistinguishability

where k is random in $\mathcal{K}$.

Intuitively, computationally indistinguishable means

indistinguishable in practice!

Definition: Two distribution ensembles $\{A_n\}_{n\in N}$ and $\{B_n\}_{n\in N}$ are

computationally indistinguishable if for any polynomial time

distinguisher D and every n,

$|Pr[D(a)=1] - Pr[D(b)=1]| = negl$

where a is sampled from A_n, b is sampled from B_n.

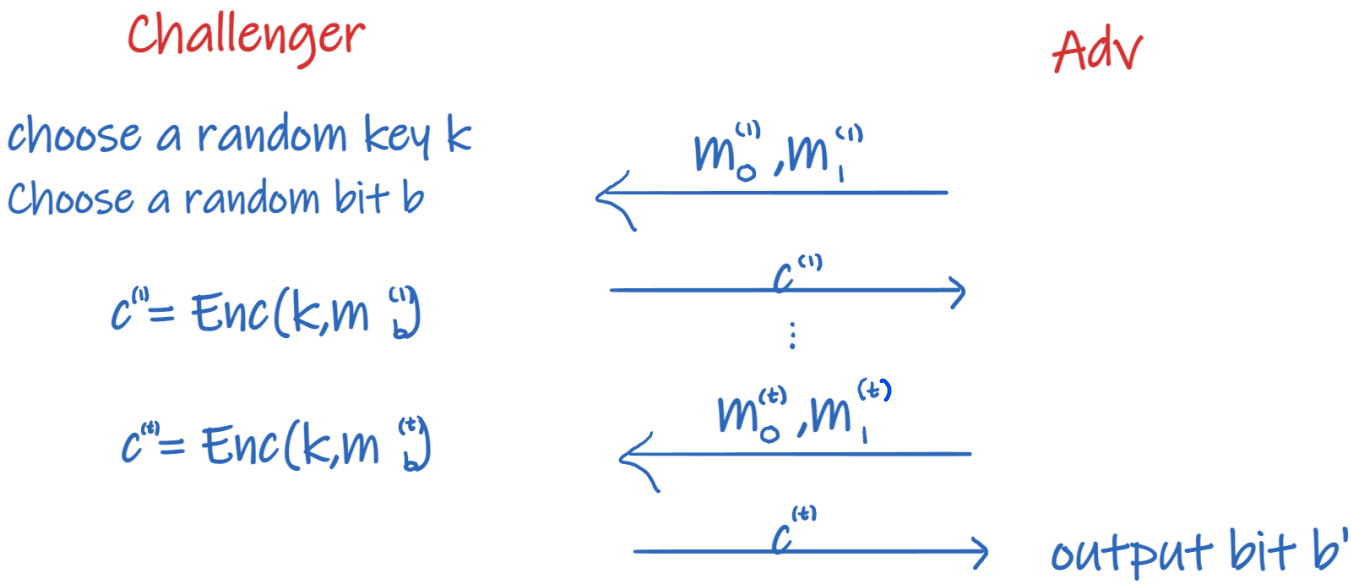
Intuitively, negl means 0 in practice.

Definition: A function μ is negligible if for every constant c in $\mathbb{N}$ there exists a constant n_c s.t. for every $n > n_c$ $\quad \mu(n) < n^{-c}$

Remark: The definition of CPA security stated above is a simplified (and weaker) form of the actual definition. In the actual definition the messages can be chosen in an adaptive manner, and the definition is a "game based" definition

Definition: Indistinguishabilty against Chosen plaintext attacks (Ind CPA, or CPA for short):

An encryption scheme (Enc, Dec) is CPA secure if every efficient adversary Adv wins in the following game with probability at most 1/2+negligible:



Adv wins if and only if b'=b.

Construction of a CPA secure encryption

Suppose: There exists a keyed function F, such that for every $x_1, x_2, \ldots, x_t$ in the domain, it holds that

$$F(K,x_1), F(k,x_2), \ldots, F(k,x_t) \cong (U, U, \ldots, U)$$

Such a function is called a pseudo-random function (PRF).

A PRF is a function that generates (fake) randomness!

Theorem: There exists a PRF assuming the existence of a one-way function

Let $f:\{0,1\}^* \longrightarrow \{0,1\}^*$ be a function.

Definition: f is a <u>one-way function</u> if it is <u>easy</u> to compute but <u>hard</u> to invert.

<u>Easy:</u> There is a poly-time algorithm that on input x outputs $f(x)$.

<u>Hard:</u> For any poly-time algorithm A there exists a negligible function μ s.t. for every n, $\Pr[A(y)=x \text{ s.t. } f(x)=y] = \mu(n)$ where the probability is over y distributed by choosing a random u in $\{0,1\}^n$ and setting $y=f(u)$.

In practice: Use AES as a PRF.

A CPA secure encryption scheme using a PRF F:

$$Enc(k,m;r) = (r, m \oplus F(k,r))$$

$$Dec(k,(r,c)) = c \oplus F(k,r)$$

The security follows from the security of the PRF and the security of the one-time pad.