Last time: RSA:

Setup: choose p, q random primes of ℓ bits ($p \neq q$)

set $n = pq$, and choose e s.t. $\gcd(e, \varphi(n)) = 1$.

"forward" direction: $m \mapsto m^e \bmod n$

for $m \in \mathbb{Z}_n$.

Also we can compute the inverse if we know p, q!

$\varphi(n) = (p-1)(q-1)$.

And since $\gcd(e, \varphi(n)) = 1$, we can compute

$$d \underset{\text{"defined as"}}{\triangleq} e^{-1} \in \mathbb{Z}^*_{\varphi(n)}.$$

(How to compute d? xgcd gives the answer!

xgcd gives $d, a \in \mathbb{Z}$ s.t. $1 = de + a\varphi(n)$

So $de \equiv 1 \bmod n$

$\therefore d = e^{-1}$)

Fact: $\forall x \in \mathbb{Z}^*_n$, then $x^{\varphi(n)} \equiv 1 \bmod n$.

Corollary: $\forall x \in \mathbb{Z}_p$, $x^p = x \bmod p$

Inverting RSA w/ knowledge of $d = e^{-1} \pmod{\varphi(n)}$:

Say (for now) that $m \in \mathbb{Z}^*_n$.

Say $c = m^e \bmod n$.

Claim: $c^d = m \bmod n$. $\left(\begin{array}{l}\text{Since } de \equiv 1 \bmod \varphi(n), \text{ for } k \in \mathbb{Z} \\ ed = k\varphi(n) + 1 \quad (\text{in } \mathbb{Z})\end{array}\right)$

$$c^d = (m^e)^d = m^{ed}$$

$$= m^{k\varphi(n)+1} = m \cdot m^{k\varphi(n)} = m \cdot (\underbrace{m^{\varphi(n)}}_{=1})^k = m.$$

Note: $m \in \mathbb{Z}_n^*$ is not necessary $((m^e)^d = m \quad \forall m \in \mathbb{Z}_n)$
but is likely true anyway: how could m fail to be in $\mathbb{Z}_n^*$? $\gcd(m,n) \neq 1$
$\gcd(m,n) \in \{1, p, q, n\}$.
So if anyone finds $m \in \mathbb{Z}_n$ w/ $\gcd(m,n) \neq 1$, they have factored n! (And thus found the secret key!)

Public key encryption attained?
(Above is an example of a Trapdoor One Way Permutation (TDP))

$M = \mathbb{Z}_n$, $SK = p, q$, $PK = (n, e)$ w/ $\gcd(e, \varphi(n)) = 1$.

$E_{PK}(m) = m^e \bmod n$. $D_{SK}(c) = c^d \bmod n$.

Recall definition of Perfect Security:

$\forall m, m' \in M, c \in C$

$$\Pr_{k \in K}[E(k,m) = c] = \Pr_{k \in K}[E(k,m') = c]$$

Another way to put it: think of $E(K,m)$ as a probability distribution on C.

(samples from $E(K,m)$ are obtained by choosing $k \in_R K$ and encrypting m.)

Then perfect security says $E(K,m) = E(K,m')$
$\forall m, m' \in M$.

$(E(K,m) : C \to [0,1])$ probability distributions on C!

RSA doesn't seem very close yet...

Imagine only messages likely to be sent are "yes" and "no".

Then RSA is a complete failure. Why?

Eve has $PK = n, e$ and thus could just compute $E_{PK}(\text{"yes"})$ & $E_{PK}(\text{"no"})$ and see which one was sent!

How to fix??

Maybe pad messages w/ randomness?

$n/2$ bits	$n/2$ bits
message	randomness

One way or another, public key encryption <u>must use randomness</u>.

See OAEP for a nice, well-analyzed version of this idea.

<u>On defining security...</u>

Analog of perfect security? Let's commit to using randomness, and make it explicit in the algos.

$$E_{PK}(m, R) \underset{PPT}{\approx} E_{PK}(m', R)$$

Probability dist. on ciphertexts!

"looks the same" to any bounded adversary. ("Computational Indistinguishability")

How to formalize?

Say $\{X_\ell\}_{\ell\in\mathbb{N}}$, $\{Y_\ell\}_{\ell\in\mathbb{N}}$ are sequences of probability distributions.

We say $X_\ell \underset{PPT}{\approx} Y_\ell$ if $\forall A \in PPT$, $\exists$ negligible func. ν s.t.

$$\left| \Pr[A(X_\ell)=1] - \Pr[A(Y_\ell)=1] \right| = \nu(\ell).$$

"A cannot behave much different on samples from X_ℓ vs samples from Y_ℓ"

Maybe A outputs "1" if it thinks it has X_ℓ samples and "0" to guess Y_ℓ.

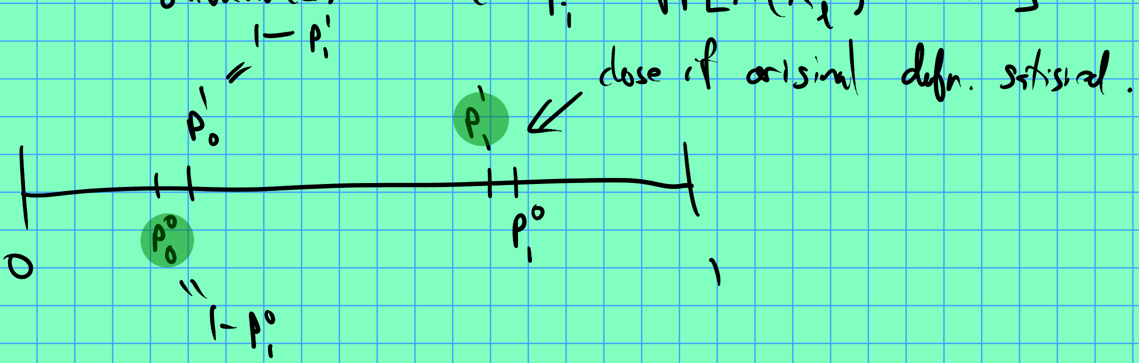
Alternate (+equivalent) defn: hard to guess.

Say distributions are $\{X_\ell^0\}$, $\{X_\ell^1\}$.

Then $X_\ell^0 \underset{PPT}{\approx} X_\ell^1$ if $\forall A \in PPT$, $\exists$ negl. function ν s.t.

$$\Pr_{b\in 0/1}[A(X_\ell^b)=b] = \frac{1}{2} + \nu(\ell).$$

How to see the equivalence: define $p_i^j = \Pr[A(X_\ell^j) = i]$



Ok. So what does it mean for A to guess correctly?

Corresponds to $\frac{1}{2}p_0^0 + \frac{1}{2}p_1^1$ (conditioning on b)

$$\Pr_{b\in 0/1}[A(X_\ell^b)=b] = \frac{1}{2}\Pr[A(X_\ell^0)=0] + \frac{1}{2}\Pr[A(X_\ell^1)=1]$$
$$= \frac{1}{2}(p_0^0 + p_1^1)$$

$$= \frac{1}{2}\Big(\underbrace{p_0^0 + p_1^0}_{=1} + \underbrace{p_1^1 - p_1^0}_{\text{negl.}}\Big) \quad \checkmark$$

Defining security for public key schemes ...

Option 1: $E_{PK}(R, m) \underset{PPT}{\approx} E_{PK}(R, m') \quad \forall\, m, m' \in \mathcal{M}.$

More concrete "game style" definition:

A $\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad$ C $\quad PK, SK \leftarrow Gen(1^\lambda)$

$A \xleftarrow{\quad PK \quad} C$

$A \xrightarrow{\quad m_0, m_1 \in \mathcal{M} \quad} C \qquad b \in_R 0/1$

$A \xleftarrow{\quad c^* = E_{PK}(m_b) \quad} C \qquad$ (Note: $|m_0| = |m_1|$)

$A \xrightarrow{\quad b' \in 0/1 \quad} C$

Say A "wins" if $b' = b$.

Say scheme is IND-CPA secure if $\forall\, A \in PPT$, $\exists\, \nu$ negl. s.t.

$$\Pr[A \text{ wins}] = \frac{1}{2} + \nu(\lambda)$$

Variations: give A more power (in the form of decryption oracles)

A $\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad$ C $\quad PK, SK \leftarrow Gen(1^\lambda)$

$A \xleftarrow{\quad PK \quad} C$

$A \xrightarrow{\quad c \quad} C$

$A \xleftarrow{\quad D_{SK}(c) \quad} C \qquad b \in_R 0/1$

$A \xrightarrow{\quad m_0, m_1 \in \mathcal{M} \quad} C$

$A \xleftarrow{\quad c^* = E_{PK}(m_b) \quad} C \qquad$ (Note: $|m_0| = |m_1|$)

$A \xrightarrow{\quad b' \in 0/1 \quad} C$

Above game is for CCA 1 (chosen cipher text attack)

A $\qquad\qquad\qquad$ C

$A \xleftarrow{PK} C$

$A \xrightarrow{c} C$

$A \xleftarrow{D_{SK}(c)} C$

$\vdots$

$A \xrightarrow{m_0, m_1 \in \mathcal{M}} C$

$A \xleftarrow{c^* = E_{PK}(m_b)} C$

$A \xrightarrow{c \neq c^*} C$

$A \xleftarrow{m = D_{SK}(c)} C$

$\vdots$

$A \xrightarrow{b' \in 0/1} C$

This is the CCA-2 game.

El Gamal Crypto system.

- IND-CPA secure under the "DDH" assumption.

Recall Diffie-Hellman key exchange:

p a prime
g a generator of $\mathbb{Z}_p^*$

Alice $\qquad\qquad\qquad$ Bob

$a \in_R \mathbb{Z}_{p-1}$ $\qquad$ $b \in_R \mathbb{Z}_p$

$\text{Alice} \xrightarrow{A = g^a} \text{Bob}$

$\text{Alice} \xleftarrow{B = g^b} \text{Bob}$

$s = A^b = g^{ab}$

$s = B^a = g^{ab}$

Idea behind El Gamal: PK is Alice's "half" of D-H.
To send a message to Alice, Bob does the other half of D-H and uses the secret to mask a message.

Details: $PK = A = g^a$, $SK = a$.

$E_{PK}(m)$, where $m \in \mathbb{Z}_p^*$ is done as follows:

choose $b \in_R \mathbb{Z}_{p-1}$, compute $B = g^b$.

Then set ciphertext $c = (B, \underbrace{A^b}_{g^{ab}} \cdot m) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$

$D_{sk}(c = (B, k))$: First, compute mask $z = B^a = g^{ab}$

Then $m = k \cdot z^{-1}$.

$\quad\quad\quad\;\; \| \quad\;\; \|$

$\quad\quad\quad m \cdot \cancel{g^{ab}} \;\; \cancel{g^{-ab}}$

Note: it actually is similar to the OTP!

$c = r \oplus m$	$r \cdot m \qquad (r = g^{ab})$
OTP	El Gamal
r is truly random	r is indistinguishable from random! ("pseudo random")

To a bounded adversary, El Gamal looks like a OTP scheme!

Here's the assumption we would like to make:

Decisional Diffie Hellman Assumption:

$$(g^a, g^b, g^{ab}) \underset{PPT}{\approx} (g^a, g^b, g^z)$$

where $a, b, z \in_R \mathbb{Z}_{p-1} \quad (p-1 = |\mathbb{Z}_p^*|)$

Bad news: DDH not quite true in $\mathbb{Z}_p^*$ ...

Reason: Legendre Symbol: you can figure out the even/oddness of a from $A = g^a$:

Say $a = 2x$ some $x \in \mathbb{Z}$.

Then $A^{\frac{p-1}{2}} = g^{a \frac{p-1}{2}} = g^{x \cdot 2 \cdot \frac{p-1}{2}} = (g^{p-1})^x = 1$.

if a odd, $A^{\frac{p-1}{2}} = -1 \quad (= p-1)$.

What to do instead? Use a large prime order <u>subgroup</u> of $\mathbb{Z}_p^*$. That is, choose random prime q

s.t. $q \cdot y + 1$ is also prime.

(so $p-1 = q \cdot y$).

Now if g generates $\mathbb{Z}_p^*$, then

$\gamma = g^{\frac{p-1}{q}}$ will generate a "subgroup" of size q in $\mathbb{Z}_p^*$.

I.e., $\gamma^0, \gamma^1, \ldots \gamma^{q-1}$ are all distinct #s in $\mathbb{Z}_p^*$,

and $\gamma^q = 1 = \gamma^0$.

For $G = \langle \gamma \rangle = \{\gamma^0, \gamma^1, \ldots\}$, DDH is conjectured to hold!

Question: try to fill in the details of fixing El Gamal using $G = \langle \gamma \rangle$ instead of $\mathbb{Z}_p^*$.

Also, read about the Chinese Remainder Theorem (CRT) before next time.