Say $M = \{0,1\}^\ell$. (like OTP)

$P \subseteq S(M)$ could be

$$P = \{ \sigma_k : m \mapsto m \oplus k \mid k \in \{0,1\}^\ell \}$$

$\forall\ x, y \in M \quad \exists$ some $\sigma \in P$ s.t. $\sigma(x) = y$.

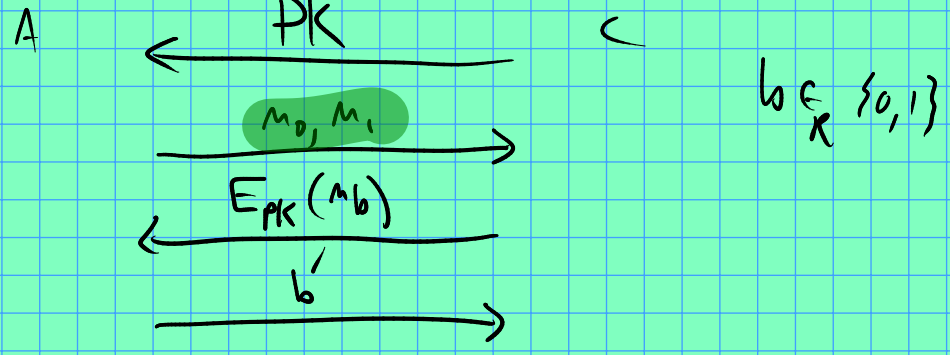
For example (OTP), set $k = x \oplus y$.

Then $\sigma_k(x) = y$.

$x \oplus k$
$= (x \oplus x) \oplus y$
$= y$

1(d): Examples of G: $\mathbb{Z}_n^*$.
Then think of $P = \{\sigma_s \mid s \in G\}$.
$\sigma_s(x) = xs$.

1(e): direct product of $\mathbb{Z}_2 \ldots$



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

Idea (II, #6): if system not secure according to "semantic" definition, then not secure according to same defn either!

$\forall\ P: M \to \{0,1\}$ $\exists$ $A \in PPT$ s.t.
A can guess $P(m)$ from $E_{PK}(m)$

How to convert A into another procedure which wins the IND-CPA game. How?

Choose m_0 s.t. $P(m_0) = 0$

and m_1 s.t. $P(m_1) = 1$.

Now give the challenge c.t. $c = E_{PK}(m_b)$

to A and see what it says.

This should give you an advantage in guessing b!

Part I, #11

What "kind" of integers might maximize $\frac{n}{\varphi(n)}$?

Bad choice: n is prime: then $\frac{n}{\varphi(n)} \approx 1$

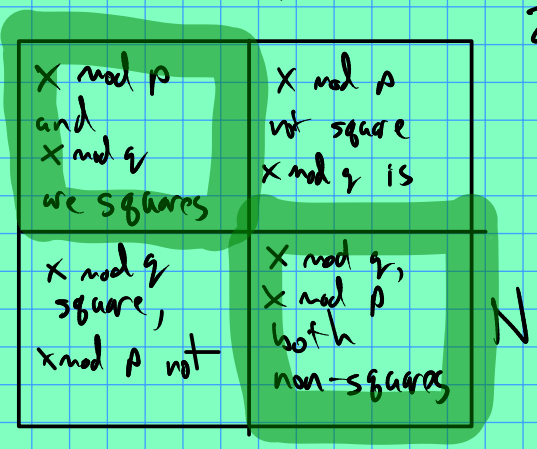
Want something "very non-prime"

Set $n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots$

can find this list using "nextprime" fn. of GMP.

Part II, #7: G-M crypto system.

set $n = pq$.



$x \in \mathbb{Z}_n^*$

"x a square mod p" $\equiv$ $x \equiv y^2 \pmod p$ for some value of y.

(Can check by looking @ $x^{\frac{p-1}{2}} \bmod p$.

$1 \Rightarrow x$ square.

$-1 \Rightarrow$ not square) $\quad -1 = p-1$

$S \equiv$ squares mod n $\quad (x \in S \Leftrightarrow \exists\, y \in \mathbb{Z}_n^*$ s.t. $x = y^2)$

Notation: define $J^+ = S \cup N$

(J for "Jacobi" + for it being +1.)

cryptosystem of G.M. 198X

Message space: $M = \{0,1\}$.

Ciphertext space: J^+

Idea: $E(0) \in_R S$. $\quad E(1) \in_R N$.

← easy: choose $y \in_R \mathbb{Z}_n^*$ and $x = y^2 \in_R S$.

← how to sample random values from N?

Assumption: $S \underset{PPT}{\approx} N$.

How to make this public key?

publish a single non square $t \in N$.

Then $PK = (n, t)$

Now we can encrypt!

$$E_{PK}(m) = x \cdot t^m \qquad (m \in \{0,1\})$$

where $x \in_R S$

(can set this as seen above: choose $y \in_R \mathbb{Z}_n^*$ and set $x = y^2$)

With knowledge of $SK = p, q$, can figure out if $c \in \mathbb{Z}_n^*$ is a square or not... ✓

Back to #): think of $\tilde{G}$ as a generator of "fake keys".

Property of "fake" keys $\tilde{pk}$: they produce ciphertexts that are impossible to decrypt:

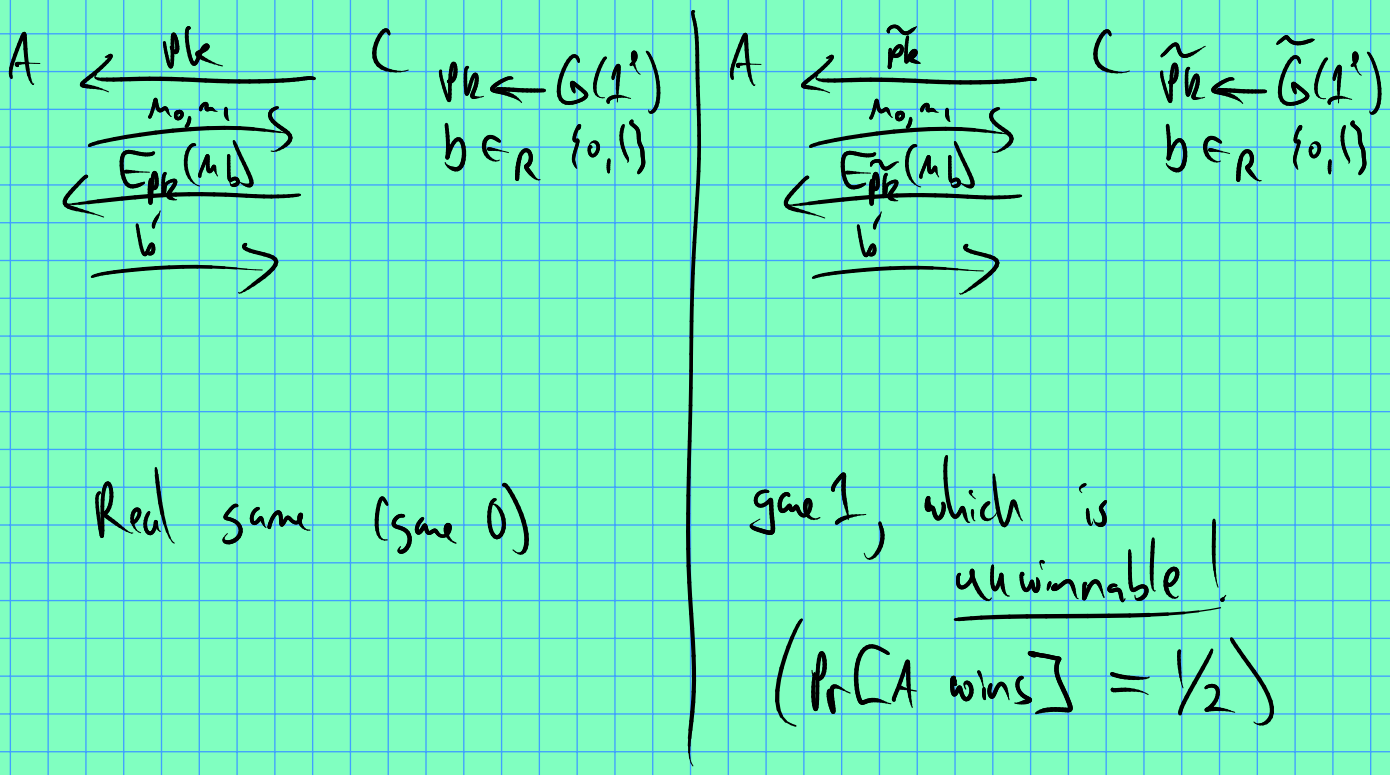
$$E_{\tilde{pk}}(m_0) \equiv E_{\tilde{pk}}(m_1) \qquad \forall\ m_0, m_1 \text{ of equal length.}$$

(equality of probability distributions)
(Just like OTP!)

in OTP, $E(m) \sim U(\{0,1\}^l) \qquad \forall\ m \in \{0,1\}^l$

To finish the argument, use a "hybrid argument":

game 0: real keys from $G(1^\ell)$.
game 1: fake keys from $\tilde{G}(1^\ell)$.



Real game (game 0)

game 1, which is unwinnable!

($\Pr[A \text{ wins}] = 1/2$)