Recall GM cryptosystem

* **Key Gen** $(1^k)$: pick random $p, q \in \mathbb{Z}$
  
  output $sk = (p, q)$, $pk = N = pq$

* **Encrypt** $(pk, m)$: pick $r \leftarrow \mathbb{Z}_N^*$

  - if $m = 0$, output $r^2 \mod N$
  - 1-bit if $m = 1$, output $-r^2 \mod N$

* **Decrypt** $(sk, c)$: if $c$ has a sqrt mod $N$, output $0$
  
  else, output $1$

Q: What unproven assumptions do we need for the GM cryptosystem to be secure?

A: Generally, for secure encrypt schemes to exist?

In general, Key Gen should "incorporate" a one-way function

**Definition**

A poly-time computable $f : \{0, 1\}^k \rightarrow \{0, 1\}^{poly(k)}$ is a one-way function (OWF) if $\exists$ PPT $A \notin \text{negl}$ s.t.

$$\Pr[x \leftarrow \{0, 1\}^k, y = f(x), x' \leftarrow A(1^k, y) : f(x') = y] \approx \frac{1}{2^k}$$
Claim: If secure PK enc schemes exist, then OWFs exist

**Proof:**
Let KeyGen be KeyGen algorithm of a secure PK enc scheme.

We want to construct a OWF \( f : \{0,1\}^k \rightarrow \{0,1\}^{\text{poly}(k')} \)

with runtime \( t(k), \text{poly in } k \)

1. Find largest \( k \) s.t. \( t(k) \leq 1 \times 1 = k' \)
2. \( f(x) \equiv \text{Run KeyGen}(1^k) \text{ using } x \) as the random tape
Output \( \text{pk} \)

OK, now proof \( f \) is a OWF

Suppose \( f \) is NOT a OWF, & let \( A \) be PPT algorithm that "breaks" \( f \).
Then use \( A \) to find \( sk' \) corresponding to \( \text{pk} \) as follows:

![Diagram showing reduction]

This is a proper reduction b/c 1. dist of input to \( A \) is what \( A \) expects
2. CORRECTNESS
3. EFFICIENCY, i.e. runs in poly-time

Question: Let \( f \) be any OWF. What about \( f(f(x)) \)? Is it necessarily a OWF?

**Attempt #1:** (INCORRECT REDUCTION)

\( f = f(x) \)

This doesn't work b/c dist to \( A \) is not what \( A \) expects
A Hard Example

This doesn't work

Because it is not correct (cond 2)

"B doesn't succeed whenever

A succeeds"

It turns out that $f(f(x))$ is not necessarily a OWF.

Proof:

Let $g: \{0,1\}^{\frac{k}{2}} \rightarrow \{0,1,2\}^{\frac{k}{2}}$ be a length-preserving OWF.

Define $f(x) = \begin{cases} o^k \circ g(x) & \text{if } x \text{ doesn't begin w/ } O^k \\ O^k \circ O^k & \text{else} \end{cases}$

where $x_i$ is first $\frac{k}{2}$ bits of $x$.

Claim: $f$ is a OWF.

Proof by contrapositive.

Suppose $A$ "breaks" $f$.

We want to construct $B$ that "breaks" $g$.

The problem is that $f(f(x))$ is always $O^k$, so finding an $x$ s.t. $f(f(x)) = O^k$ is trivial.
Input to $A$ "in the wild": Inside $B$:

$$x \leftarrow \{0,1\}^k \quad \text{is the all}
$$

if $x$ begins w/ $\frac{k}{2}$ zeros string

give $A$, ok

don't know

else
give $A$ $0^{\frac{k}{2}} \circ g(x)$

run $A$ on $0^{\frac{k}{2}} \circ g(x)$

so, dist to $A$ inside $B$ is not identical to that in the wild

but, fortunately, the dists are $\text{STAT.~CLOSE!}$

↓

so cond. 1 is met

Now for correctness,
We know that the prob $A$ succeeds is some non-negl $\varepsilon$.

$\varepsilon(k) = \text{Pr}[A \text{ succeeds}] = \text{Pr}[A \text{ succeeds & } x \text{ is the all zero string}]

+ \text{Pr}[A \text{ succeeds & } x \text{ isn't the all zero string}]$

$\text{non-negl}$.

$\text{Pr}[B \text{ succeeds}] \geq \text{Pr}[B \text{ succeeds & } x \text{ is "good"}] = \text{non-negl}$

Finally, $B$ also runs in poly-time

Assumptions:

A1 Factoring is hard

A2 OWFs exist

A3 GM crypto sys is secure

A4 Secure cryptosys exist

Impagliazzo's world:

1. Pessiland: $P \neq \text{NP}$ but OWFs don't exist

2. Minicrypt: OWFs exist but PK crypto doesn't

3. Cryptomania: PK ens & beyond!