Lecture 37: Signature of Long Messages
Let $\mathcal{F} = \{f_1, f_2, \ldots, f_\alpha\}$ be a family of functions from $\mathcal{D} \to \mathcal{R}$ (if $f_i$s are permutations, then $\mathcal{D} = \mathcal{R}$).

Let $T = \{\text{trap}_1, \text{trap}_2, \ldots, \text{trap}_\alpha\}$ be the set of corresponding trapdoors for these functions.

It is difficult to invert the functions $f_i$.

However, given $\text{trap}_i$, the function $f_i$ is easy to invert.

We saw how these trapdoor OWF/OWP families can be used to construct public-key encryption and digital signatures.
Public-key Encryption.

**Alice**

\[ r \leftarrow \mathcal{D} \]

\[ y = f_i(r) \]

\[ c = m \cdot r \]

**Bob**

Randomly generate \((pk, \text{trap}) = (i, \text{trap}_i)\)

\[ \tilde{c} = f_i^{-1}(y; \text{trap}_i) \]

\[ \tilde{m} = c \cdot (\tilde{r})^{-1} \]
Using the RSA assumption, the functions are $x^e$, for $e \in \mathbb{Z}_{\varphi(N)}^*$.

The corresponding trapdoor is $d$ such that $e \cdot d \equiv 1 \pmod{\varphi(N)}$. 

Signature
Digital Signature. based on RSA assumption

Alice

Generate $(N, e, d)$ and random $r$

$\sigma = (r\|m)^d$

Bob

$\text{pk} = (N, e, r)$

$(m, \sigma)$

$(\sigma)^e == (r\|m)$

Intuitively, Alice picks a function $f_e$ by choosing $e$. Then, the signature on $(r\|m)$ is $\sigma = f_e^{-1}(r\|m) = (r\|m)^d$. Verification if performed by checking $f_e(\sigma) == (r\|m)$. 
Suppose the integers in $\mathbb{Z}_N^*$ need $2n$-bits to be expressed.

Then, our scheme signs messages $m$ of length $n$-bits, using a signature $\sigma$ of length $2n$-bits.

Can we sign long messages using a small signature?
The intuition here is to hash down the message using a collision-resistant hash function family, and then sign the hash.

Let \( H = \{ h_1, h_2, \ldots, h_β \} \) be a family of collision-resistant hash functions from the domain \( \{0, 1\}^* \rightarrow \{0, 1\}^n \)

**Alice**

Generate \((N, e, d)\) and random \(r\) and \(sk\)

\[ \sigma = (r \| h_{sk}(m))^d \]

**Bob**

\[ pk = (N, e, r, sk) \]

\[ (m, \sigma) \rightarrow (\sigma)^e = (r \| h_{sk}(m)) \]