Today:

- Signatures:
  * Recall definition
  - Hash & Sign paradigm
  - RSA signatures & full domain hash
  - El-Gamal signature scheme
Security:

Def: Existential unforgeability against adaptive chosen message attacks:

(i) Challenger generates \((pk, sk) \leftarrow \text{KeyGen}(1^\lambda)\)

(ii) Adversary obtains oracle access to \(\text{Sign}(sk, \cdot)\)

(iii) Adversary outputs a pair \((m, \sigma)\)

Adversary wins if

- \(\text{Verify}(pk, m, \sigma) = 1\)
- \(m \in \{m_1, \ldots, m_g\}\)

Def: A scheme is \underline{secure} (i.e., existentially unforgeable against adaptive chosen msg attacks) if

\[ Pr[\text{Adv wins}] = \text{negl}(\lambda) \]

Def: A scheme is \underline{strongly secure} if adv cannot even produce a new signature for a msg that was
previously signed for him.

Namely, adv wins if

- \( \text{Verify}(pk, m, \sigma^w) = 1 \)
- \((m, \sigma^w) \notin \{ (m_1, \sigma_1), \ldots, (m_g, \sigma_g) \}\)

\underline{Hash & Sign :}

For efficiency reasons, often better to use sign \( h(msg) \) rather than \( msg \) (where \( h \) is a cryptographic hash function), since hashing (say, SHA-256) is extremely efficient compared to signing operations (such as modular exponentiations).

* Hash function needs to be collision resistant!

\underline{Claim :} If \(( \text{KeyGen}, \text{Sign}, \text{Verify}) \) is secure \& \( H = \{ h_k \} \) is collision resistant hash family, then the hash & sign version of \(( \text{KeyGen}, \text{Sign}, \text{Verify}) \) is also secure.

\underline{Interestingly :} Hash & Sign paradigm is also useful for security!
Signing with RSA

Diffie & Hellman (1976) suggested a (general) method for using a deterministic public-key encryption scheme as a signature scheme:

**Idea:** \( \text{Sign}(sk, m) = \text{Dec}(sk, m) \)

\[ \text{Verify}(pk, m, \sigma) = 1 \text{ iff } \text{Enc}(pk, \sigma) = m \]

**Signing with RSA: First Attempt**

**KeyGen(1^n):** Choose \( n = p \cdot q \) random 2-bit primes.

Choose \( e, d \) random s.t. \( e \cdot d = 1 \mod \phi(n) \).

\( PK = (n, e) \)

\( SK = (n, d) \)

\[ \text{Sign}(sk, m) = m^d \mod n \]

\[ \text{Verify}(pk, m, \sigma) = 1 \text{ iff } \sigma^e = m \mod n \]

**Correctness**

\( m \in \mathbb{Z}_n \)

\[ (m^d)^e = m^{de} = m \mod n \]

\( \checkmark \)
Is this secure? No!

Given \( \text{Sign}(sk, m) = m^d \mod n \)

one can easily \( \text{sign} \ m^2 \mod n \).

Idea: Use hash & sign

\[ \text{Sign}((sk, h), m) = (h(m))^d \mod n. \]

\[ \text{Verify}((pk, h), m, \sigma) \iff \sigma^e = h(m) \mod n. \]

Is this secure??

Depends on \( h \ldots \)

Bellare-Rogaway 93:

"Random oracles are practical: a paradigm for designing efficient protocols."

Introduced ROM (Random Oracle Model).

[BR93] Proved that Hash & Sign RSA (a.k.a full domain hash, FDH) is secure in the ROM assuming RSA assumption (i.e., RSA is hard to invert on avg). (Generalizes to any trapdoor permutation..."
Security reduction is not tight...

Loosely speaking, if RSA function is \((t', \varepsilon')\)-secure (i.e. \(\mathcal{A}_{\text{adv}}\) running in time \(t'\) can invert w.p. \(\leq \varepsilon'\))

then FDH scheme is \((t, g_{\text{sig}}, g_{\text{hash}}, \varepsilon)\)-secure

(i.e., \(\mathcal{A}_{\text{adv}}\) running in time \(t\), making \(\leq g_{\text{sig}}\) signature calls

& \(\leq g_{\text{hash}}\) hash calls, can forge a new signature w.p. \(\leq \varepsilon\)

where:

\[
t = t' + \text{poly}(g_{\text{sig}}, g_{\text{hash}}, \sigma)
\]

\[
\varepsilon = (g_{\text{sig}} + g_{\text{hash}}) \cdot \varepsilon'
\]

---

**Probabilistic Signature Scheme (PSS)**

[Bellare-Rogaway 96]

RSA-based signature scheme secure in the ROM with tighter security proof.

\[
m, r \xrightarrow{\text{encoding}} y \xrightarrow{f} y^d \mod n
\]
El-Gamal Signatures

Note: The paradigm $\text{Enc}((\text{Dec}(m)))$ doesn’t work for El-Gamal, since El-Gamal is not a trapdoor permutation (it is randomized).

**Scheme**

- $\mathbb{P} \mathbb{P}$: prime $\mathbb{p}$
  
  \[ g \text{ generator of prime order subgroup } \mathbb{g}, \text{ order } \mathbb{g}/\mathbb{p}-1 \]

**KeyGen**

- $x \leftarrow \mathbb{Z}_\mathbb{g}$
  - $\mathbb{s} \mathbb{k} = x$
  - $\mathbb{y} = g^x \mod \mathbb{p}$
  - $\mathbb{p} \mathbb{k} = \mathbb{y}$

**Sign($\mathbb{p} \mathbb{P}, \mathbb{sk}, m)$**:

- Choose $\mathbb{k} \leftarrow \mathbb{Z}_\mathbb{g}^*$

- Output $(\mathbb{r}, \mathbb{s}) = (g^k \mod \mathbb{p}, \frac{h(m) + rx}{k} \mod \mathbb{g})$

**Verify($\mathbb{p} \mathbb{P}, \mathbb{PK}, m, (\mathbb{r}, \mathbb{s}))$**:

- Check that $0 < r < \mathbb{p}$

- Check that $y^{r/s} \cdot g^{h(m)/s} = r$
Correctness:
\[ y^{r/s} \cdot g^{h(m)/s} = g^{\frac{xr + h(m)}{s}} = g^k = r \mod p \]

Security:
- Insecure with \( h = \text{identity} \) (exercise).
- Not known to be secure in ROM
- Secure in ROM if \( h(m) \) is replaced with \( h(m||r) \)

[Pointcheval - Stern 96]:
[Intuition: If \( h(m||r) \) then adversary needs to choose \( r \) and succeed for many values of \( h(m||r) \).
\( \Rightarrow \) knowledge of \( k \). \( \Rightarrow \) knowledge of \( s \).

Thm: Modified El-Gamal is existentially unforgeable against adaptive chosen msg attacks in ROM, assuming DLP is hard (on avg).

Digital Signature Standard
(DSS - NIST 91)

Public Parameters: \( p \) prime, \( q \mid p - 1 \)
\[ \|p\| = 1024 \text{ bits}, \quad \|q\| = 160 \text{ bits} \]
\( g \) generator of subgroup of \( \mathbb{Z}_p^* \) of order \( q \).
**KeyGen**: $x \leftarrow \mathbb{Z}_p^*$  
$y = g^x$  
$PK = y$  
$|y| = 1024$ bits

**Sign_{sk}(m)**: $y \leftarrow \mathbb{Z}_p^*$  
$r = (g^x \mod p) \mod q$  
$|r| = 160$ bits

$$S = \frac{h(m) + rx}{g^y} \mod q$$  
$|S| = 160$ bits

Redo if $r = 0$ or $S = 0$

Output $(r, S)$.

**Verify_{pk}(m, (r, S))**:  
- Check $0 < r < q$
- Check $y^{r/s} \cdot g^{h(m)/s} \equiv g^{rx+h(m)/s} \mod p \equiv g^r \mod q$

**Correctness**: $y^{r/s} g^{h(m)/s} = g^{(x \cdot r + h(m))/s} = g^r = r \mod p \mod q$.

**Security**: As before, provably secure if $h(m)$ is replaced with $h(m||r)$. 