Cryptography
CS 555

Topic 21: Digital Schemes (1)
Outline and Readings

- Outline
  - Digital signature
  - RSA signatures
  - Hash and sign

- Readings:
  - Katz and Lindell: Chapter 12.1-12.4
Digital Signatures: The Problem

- Consider the real-life example where a person pays by credit card and signs a bill; the seller verifies that the signature on the bill is the same with the signature on the card.
- Contracts are valid if they are signed.
- Signatures provide non-repudiation.
  - ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract.
- Can we have a similar service in the electronic world?
  - Does Message Authentication Code provide non-repudiation? Why?
Digital Signatures

- MAC: One party generates MAC, one party verifies integrity.
- Digital signatures: One party generates signature, many parties can verify.
- Digital Signature: a data string which associates a message with some originating entity.
- Digital Signature Scheme:
  - a signing algorithm: takes a message and a (private) signing key, outputs a signature
  - a verification algorithm: takes a (public) verification key, a message, and a signature
- Provides:
  - Authentication, Data integrity, Non-Repudiation
Digital Signature

- A signature scheme consists of the following three PPT algorithms
  - \((pk, sk) \leftarrow \text{Gen}(1^n)\) key generation
  - \(\sigma \leftarrow \text{Sign}_{sk}(m)\) signing
  - \(b := \text{Vrfy}_{pk}(m, t)\) verification algorithm
    - \(b=1\) meaning valid, \(b=0\) meaning invalid

Must satisfy \(\forall (pk, sk) \forall m \text{Vrfy}_{pk}(m, \text{Sign}_{sk}(m)) = 1\)

Assume that receiver has an authentic copy of the sender’s public key, then receiver can verify that a document is indeed sent by the sender.
Security of Signature Schemes

• The experiment $\text{Sig-forg}_{A,\Pi}$
  – $(pk,sk) \leftarrow \text{Gen}(1^n)$
  – Adversary $A$ is given $pk$ and oracle access to $\text{Sign}_{sk}(\cdot)$
  – Adversary outputs $(m, \sigma)$. Let $Q$ denote the set of all queries that $A$ asked to the oracle.
  – Adversary wins if $\text{Vrfy}_{pk}(m, t) = 1$ and $m \notin Q$

• A signature $\Pi$ is existential unforgeable under an adaptive chosen-message attack (or just secure) if for all PPT $A$, there exists a negligible function $\text{negl}$ such that
  $\Pr[\text{Mac-forg}_{A,\Pi}=1] \leq \text{negl}(n)$
“Textbook RSA” Signatures

Key generation (as in RSA encryption):

Public key: \((e, n)\) used for verification
Private key: \(d\) used for generation

Signing message \(m\) with private key

- Compute \(\sigma = m^d \mod n\)

Verifying signature \(\sigma\) using public key \((e, n)\)

- Check whether \(\sigma^e \mod n = m\)
Insecurity of “Textbook RSA”

- A no-message attack
  - Choose arbitrary $\sigma$, compute $m = \sigma^e \mod n$
  - $(m, \sigma)$ is a valid pair
  - One cannot control what is $m$

- Forging signature on arbitrary message
  - To forge signature on message $m$, query signing oracle for $m_1$ (obtaining $\sigma_1$) and $m_2 = m/m_1 \mod n$ (obtaining $\sigma_2$)
  - $(m, \sigma_1 \sigma_2)$ is a valid pair
RSA Signatures with Hash

Use a hash function $H: \{0,1\}^* \rightarrow \mathbb{Z}_n^*$

Signing message $m$ with private key $(n,d)$
- Compute $\sigma = H(m)^d \mod n$

Verifying signature $\sigma$ using public key $(e, n)$
- Check whether $\sigma^e \mod n = H(m)$

Can be proven secure assuming that $H$ is random oracle. (This is not considered a valid proof of security, but means that no known attack exists.)
Hash and Sign Paradigm

- Enabling the signing of arbitrary long message.

- Given a secure signing scheme (for a fixed message space), and a collision-resistant hash function, first hash and then sign is also secure.
  - "Textbook RSA" is insecure, so this result does not apply to hash and sign with RSA
  - Any attack either finds a collision or breaks the security of the signing scheme.
Non-repudiation

- Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

- Can one deny a signature one has made?

- Does email provide non-repudiation?
Coming Attractions …

- Other Signature Schemes
- Reading: Katz & Lindell: Chapter 12.5, 12.7