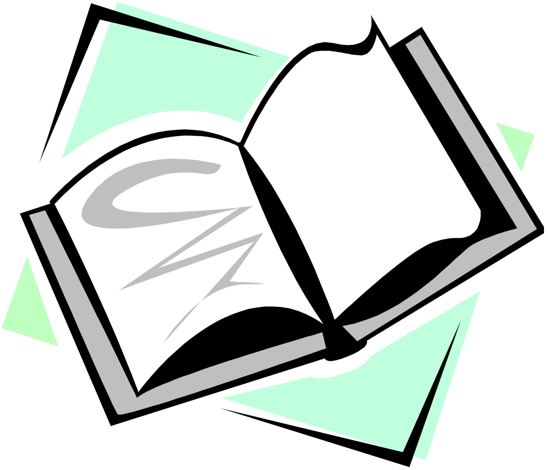
Cryptography
CS 555

Topic 22: Digital Schemes (2)

Outline and Readings

- Outline
  - The DSA Signature Scheme
  - Lamport’s one-time signature
  - Blind signature

- Readings:
  - Katz and Lindell: Chapter 12.1-12.4



Digital Signature Algorithm (DSA)

Also known as Digital Signature Standard (DSS)

Key generation

- Select two prime numbers (p,q) such that q | (p-1)
- Early standard recommended p to be between 512 and 1024 bits, and q to be 160 bits
- Current recommendation for length: (1024,160), (2048,224), (2048,256), and (3072,256).
  - The size of q must resist exhaustive search
  - The size of p must resist discrete log
- Choose g to be an element in Z_p^* with order q
  - Let α be a generator of Z_p^*, and set $g = \alpha^{(p-1)/q} \bmod p$
- Select $1 \leq x \leq q-1$; Compute $y = g^x \bmod p$

Public key: (p, q, g, y)

Private key: x

DSA

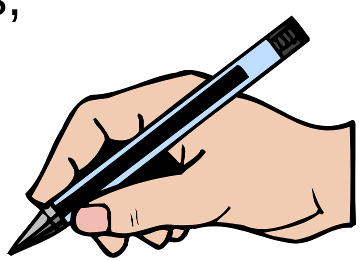
Signing message M:

- Select a random integer k, $0 < k < q$
- Compute

$$r = (g^k \bmod p) \bmod q$$

$$s = k^{-1} (h(M) + xr) \bmod q$$

- Signature: (r, s)
  - Signature consists of two 160-bit numbers, when q is 160 bit



DSA

Signature: (r, s)

$r = (g^k \bmod p) \bmod q$

$s = k^{-1} (h(M) + xr) \bmod q$

Verification

- Verify $0 < r < q$ and $0 < s < q$, if not, invalid
- Compute

  $u_1 = h(M)s^{-1} \bmod q$,

  $u_2 = rs^{-1} \bmod q$
- Valid iff $r = (g^{u_1} y^{u_2} \bmod p) \bmod q$

  $g^{u_1} y^{u_2} = g^{h(M)s\text{^}\{-1\}} g^{xr\ s\text{^}\{-1\}}$

  $= g^{(h(M)+xr)s\text{^}\{-1\}} = g^k \pmod p$

DSA Security

- The value k must be unique and unpredictable.
- No security proof exists, even assuming that the hash function is a random oracle.
- No vulnerability known either.
- Adopted as standard in 1991
  - Main benefits over RSA, which helps its adoption, are
    - One cannot use the implementation for encryption
    - Signature size (320 bit) is smaller than RSA

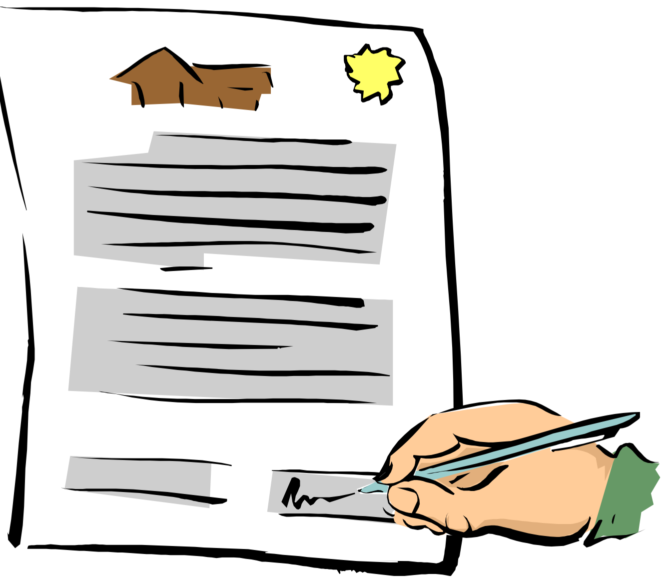
One-Time Digital Signatures

- One-time digital signatures: digital schemes used to sign,at most one message; otherwise signature can be forged.
- A new public key is required for each signed message.
- Advantage: signature generation and verification are very efficient and is useful for devices with low computation power.

Lamport One-time Signature

To sign one bit:

- Choose as secret keys x_0, x_1
  - x_0 represents ‘0’
  - x_1 represents ‘1’
- public key (y_0,y_1):
  - $y_0 = f(x_0)$,
  - $y_1 = f(x_1)$.
  - Where f is a one-way function
- Signature is x_0 if the message is 0 or x_1 if message is 1.
- To sign a message m, use hash and sigh each bit of h(m)



Blind Signature Schemes

- A wants B's signature on a message m, but doesn't want B to know the message m or the signature
- Applications: electronic cash
  - Goal: anonymous spending
  - The bank signs a bank note, but A doesn't want B to know the note, as then B can associate the spending of B with A's identity

Chaum's Bind Signature Protocol Based on RSA

- Setup:
  - B has public key (n,e) and private key d
  - A has m
- Actions:
  - (blinding) A picks random $k \in Z_n - \{0\}$ computes $m' = mk^e \bmod n$ and sends to B
  - (signing) B computes $s' = (m')^d \bmod n$ and sends to A
  - (unblinding) A computes $s = s'k^{-1} \bmod n$, which is B's signature on m

Coming Attractions …

- In the next two weeks
  - Zero knowledge proof protocols
  - Commitment schemes
  - Secure function evaluation, Oblivious transfer, secret sharing
  - Identity based encryption & quantum cryptography
- We will be using materials not in the textbook