Digital Signatures

Monday, November 17, 2025 9:21 AM

Recall: Public-key systems
private-key → to sign
pub-key → to verify

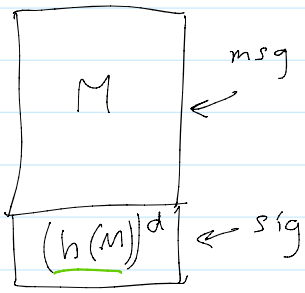
Missing
100 # 3, 6, 7, 8, ~~10~~ 12, 17
200 # 11, 19, 23, 24, 25,

1] Digital Signature (idea)
① To sign message M, we actually sig the message digest $m = h(M)$
② use the pri-key to sign m
③ use h(M) and the pub-key to verify the sig.

2] RSA Signature

To sign $m = h(M)$

① $m = h(M) < n = p \cdot q$
② $s = m^d \pmod n$
$= (h(M))^d \pmod n$



To verify $(m = h(M), s)$

① $m = h(M)$

② check $s^e \equiv m \pmod n$

3] e.g. Alice public-key is $(e=3, n=55)$, $p=5, q=11$

① Find pri-key:
$d \equiv e^{-1} \pmod{\varphi(n)}$
$\equiv 3^{-1} \pmod{40} \equiv (-13) \equiv 27 \pmod{40}$

② Sign $m = h(M) = 5$

$5 = 5^{27} \pmod{55}$

$\equiv 25 \pmod{55}$

③ verify $(m = 5, \quad s = 25)$

check $s^e = m \pmod{n}$

$s^e = 25^3 \equiv 5$ ✓

$\therefore$ Valid sig.

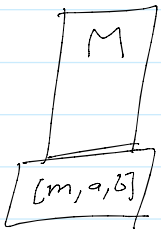
4] El Gamal Digital Signature

Setups:

- $\mathbb{Z}_p^*$, with large prime p
- generator: $\langle g \rangle = \mathbb{Z}_p^*$
- keys: private-key: $x \in \mathbb{Z}_p^*$, $x < p$
  pub-key: (g, y, p); $y = g^x$

5] Signing a message (digest) $m = h(M) \in \mathbb{Z}_p^*$

- The sig is of the form $[m, a, b]$ that can be generated by Alice who holds the pri-key
- the sig can be verified publicly.



6] To sign $m = h(M)$

① choose a random r co-prime to $\varphi(p) = p-1$ and compute: $a = g^r$

② Solve for b in: $m = xa + rb \pmod{\varphi(p)}$

$\Rightarrow b = (m - xa) \cdot r^{-1} \pmod{\varphi(p)}$

③ Sig $= [m, s_1 = a, s_2 = b]$

7] To verify : $[m, a, b]$

check : $g^m = y^a \cdot a^b$

$g^m = g^{xa} \cdot g^{rb}$

$= y^a \cdot a^b$

Proof:

$$g^m = g^{xa+rb}$$

$$= g^{xa} \cdot g^{rb}$$

$$= (g^x)^a \cdot (g^r)^b$$

$$= y^a \cdot a^b$$

8] e.g. $p = 11$, $g = 2$, $x = 3$

1. Sig $m = h(M) = 6$

① choose $r = 4$ ✗ not co-prime to 10

$r = 7$

$\Rightarrow a = g^r = 2^7 = 7 \pmod{11}$

② Solve for b in: $m \equiv xa + rb \pmod{p-1}$

$\Rightarrow b \equiv (m - xa) \cdot r^{-1} \pmod{p-1}$

$\equiv (6 - 3 \cdot 7) \cdot 7^{-1} \pmod{10}$

$\equiv 5 \cdot 3$

$\equiv 5 \pmod{10}$

③ $Sig = [6, s_1 = 7, s_2 = 5]$

2. Find the pub-key:

$y = g^x \equiv 8 \Rightarrow (11, 2, 8)$

3. Verify: Sig $[m=6, a=7, b=5]$

check: $g^m = y^a \cdot a^b$

$$g^m \equiv 2^6 \equiv 9$$

$$y^a \cdot a^b \equiv 8^7 \cdot 7^5$$

$$\equiv 9 \checkmark$$

$\Longrightarrow$ Valid sig.

9] Security Issues:

① Randomness: Same M can be signed differently by the same person using different r.

② r must be kept secret. why?
knowing r $\Rightarrow$ solving for x in $m = xa + rb$

③ r should not be re-used to sig different messages.

Given $[m_1, a, b_1]$
$[m_2, a, b_2]$ Same a.

Eve solve: $m_1 = xa + r b_1$, $m_2 = xa + r b_2$ $\Longrightarrow$ solve x and r

---

Quiz:

1. $\mathbb{Z}_{15}^*$

7

1, 2, 4, 8, 11, 13, 14

#2.

$123456 \equiv 56524 \pmod{11}$

$3 \quad - \quad 2 \quad = 6$

#3. $140 = 2^2 \cdot 5 \cdot 7$

$3 \cdot 2 \cdot 2 = 12$ divisors.

#4. $104 = \cdots\cdots$

$5 = 1 \cdot 4 + 1 \leftarrow$ gcd.

$\vdots$

$1 = 2 \cdot 104 - 23 \cdot 9$ 3 pts.

$\therefore 9^{-1} \equiv -23 \equiv ?$ (-1)

$\equiv 81$ ✓ 1,