08160671 李明澤

1) Now consider the opposite problem: using an encryption algorithm to construct a one-way hash function. Consider using RSA with a known key. Then process a message consisting of a sequence of blocks as follows: Encrypt the first block, XOR the result with the second block and encrypt again, etc. Show that this scheme is not secure by solving the following problem. Given a two-block message B1, B2, and its hash

$$\mathrm{RSAH}(\mathrm{B1}, \mathrm{B2}) = \mathrm{RSA}(\mathrm{RSA}(\mathrm{B1}) \oplus \mathrm{B2})$$

Given an arbitrary block C1, choose C2 so that $\mathrm{RSAH}(\mathrm{C1}, \mathrm{C2}) = \mathrm{RSAH}(\mathrm{B1}, \mathrm{B2})$.
Thus, the hash function does not satisfy weak collision resistance.

$RSAH(C_1, C_2)$

$= RSA(RSA(C_1) \oplus C_2)$

$[\ RSA(RSA(B1) \oplus B_2)\ ]$

$\Rightarrow RSA(RSA(C1) \oplus \underbrace{RSA(C1) \oplus RSA(B1) \oplus B_2}_{= C_2})$

$= RSA(0 \oplus RSA(B_1) \oplus B_2)$

$= RSAH(B_1, B_2)$

$C_2 = RSA(C1) \oplus RSA(B1) \oplus B_2$

2) DSA specifies that if the signature generation process results in a value of s = 0, a new value of k should be generated and the signature should be recalculated. Why?

$s = 0 = [k^{-1}(H(M) + xr)] \mod q$

$x = \frac{-H(M)}{r} \mod q$

↳ private key

---

3) Compute the signature of M="Hello!" using the specified methods, where H(W)=last 4 bits of SHA256(W) for a binary string W. Also, compute the corresponding public keys and verify correctness of the signatures.

a) RSA: n=323=17x19, private key=(323, 7^{-1} mod 288).
b) ElGamal: q=103, α=11, private key X_A=35.
c) Schnorr: p=103, q=17, a=72, private key = (103, 17, 72, 10)
d) DSA: p=103, q=17, g=72, private key = (103, 17, 72, 7)

7 ⇓ 0111

(a) Sign $M \Rightarrow (M, S)$

$m = H(M) = 7$

$S = m^d \mod n$

$= 7^{247} \mod 323 = 216 \Rightarrow (M, 216)$

Verify: $PU = (323, 7)$

$m = 7$

$m' = S^e \mod n$

$= 216^7 \mod 323$

$= 7 = m$ Verified!

(b) Elgamal: $q = 103$, $\alpha = 11$, private key $X_A = 35$

$PU = (103, 11, Y_A)$, $Y_A = 11^{35} \bmod 103 = 101$

Sign $M = (M, S_1, S_2)$, $m = 7$

choose $k = 5$

$S_1 = \alpha^k \bmod q = 11^5 \bmod 103 = 62$

$S_2 = k^{-1}(m - X_A S_1) \bmod (q-1)$

$= 41 \cdot (-263) \bmod 102 = 57$

$\Rightarrow (M, 62, 57)$

Verify: $\alpha^m \bmod q$

$= 11^7 \bmod 103 = 86$

$Y_A^{S_1} S_1^{S_2} \bmod q$

$= 101^{62} \cdot 62^{57} \bmod 103$

$= 91 \cdot 10 \bmod 103$

$= 86 = \alpha^m \bmod q$ Verified!

(c) Schnorr: $p=103$, $q=17$, $a=72$ PR = (103, 17, 72, 10) (p, q, a, s)

$PU = (p, q, a, v)$, $v = a^{-s} \bmod 103$

$\Rightarrow (103, 17, 72, 66)$ $= 72^{-10} \bmod 103$

$\Rightarrow 72^{17} \bmod 103$

$= 66$

Sign M: (e, y)

$m = 17$

choose $r = 1$

$x = a^r \bmod p$

$= 72^1 \bmod 103 = 72 = H$ (Ascii)

$e = H(M \| x) = 12$

$y = (r + se) \bmod q$

$= (1 + 120) \bmod 17$

$= 2$

$\Rightarrow (12, 2)$

Verify:

$x' = a^y v^e \bmod p$

$= 72^2 66^{12} \bmod 103$

$= 34 \cdot 93 \bmod 103$

$= 72 = H$ (Ascii)

$H(M \| x') = 12 = e$ Verified!

(d) DSA: $p=103$ $q=17$ $g=72$ $x=7$ PR: $(103, 17, 72, 7)$

$y = g^x \bmod p = 72^7 \bmod 103 = 66$ (PU)

Sign M: (r, s)

choose $k = 1$, $m = 7$

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

$= (72^1 \bmod 103) \bmod 17$

$= 72 \bmod 17$

$= 4$

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

$= 18(7 + 7 \cdot 4) \bmod 17$

$= 1$

$\Rightarrow (4, 1)$

Verify:

$w = (s')^{-1} \bmod q$

$= 1^{-1} \bmod 17 = 1$

$u_1 = [H(M')\, w] \bmod q$

$= 7 \cdot 1 \bmod 17 = 7$

$u_2 = r' w \bmod q$

$= 4 \cdot 1 \bmod 17 = 4$

$v = [(g^{u_1} y^{u_2}) \bmod p] \bmod q$

$= [72^7 \, 66^4 \bmod 103] \bmod 17$

$= 72 \bmod 17$

$= 4 = r'$

Verified!

4) Use the DFT method to factor M=77 by choosing a=8, m=7, n=12. Use a tool, such as Matlab, to compute DFT. You need to show all steps of computation.

$M = 77 = 7 \times 11$

$a = 8$

$f_{a,M}(x)$ has the period $S = 60$ ($8^{60} \bmod 77 = 1$)

calculate the $z = \frac{d_i}{N}$ and select the most frequently occuring denominator and find the lcm (2.4.5.6)

$8^{30} \bmod 77 = 1$

$\Rightarrow 8^{15} \bmod 77 = 43$

$\gcd(42, 77) = 7$ (11 p)

$\gcd(44, 77) = 11$ (4 q)