08/6067 李明潭

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

$$RSAH(B1,B2) = RSA(RSA(B1) \oplus B2)$$

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

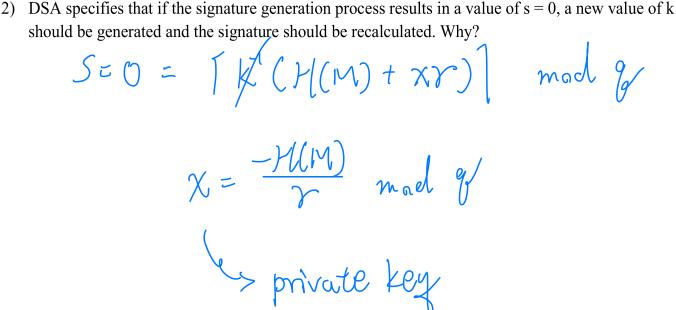
RSAH(C_1 , C_2)

= RSA(RSA(C_1) \oplus C_2)

RSA(RSA(B_1) \oplus B_2)

=> RSA(RSA(C_1) \oplus RSA(C_1)

Cz = RSA(cl) @ RSA(Bl) @ Bz



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.

ULL

- a) RSA: n=323=17x19, private key=(323, 7⁻¹ mod 288).
- b) ElGamal: q=103, $\alpha=11$, 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)

(b) Elgament: 8=103, d=11, private key X=35 PU=(103, 11, YA), YA= 1135 wad 603 =10/ Sign M= (M. 51, 52), m= 7 choose k=5 Si = 2k mod 9/ = 115 nod 103 = 62 S2 = K (m- XAS1) mad(9)-1) = 41. (2163) mad 102 = 57 => (M, 62, 51) Verify: 2 mad 9/ = 11 mad 103 = 86 Yasi mad g = 10/62 · 62 57 mod 103 = 91 · 10 mod 103 = 86 = 2 mod of Verified!

```
(C) Schnor: p=103, 9/=17, a=12 PR2(103, 17, 12,10)
     DU=Cp, q, a, v), v= a-3 mad 133
       => (203, 17, 72,66) = 72<sup>-10</sup> mod 103
                            => 12 mad 103
   Sign 14: (e,y)
                              = 66
    m= 1
   choose ral
                                           11 40
    X= ar mod P
     = 12 mad (03 = 12 = H (Ascii)
    e=HCM||x)=12
    y = (rt 50) mod 9/
      = (1+ 120) mad M
    => (12,2)
    Verify:
      x = at v mad p
       = 12 66 mod 103
       2 34.93 mod 103
        > 12 = H (Ascii)
     H(M|x')=12 = e Verified!
```

cd DSA: p=103 7=17 7=12 PR:(103,17,12,7) y= gx mad p = 12 mad 603 = 66 (PU) Sogn M: (r,5) choose k= 1, m=1 r= (gk mad p) mod g/ = (12 mad 603) mad 17 = 12 mod M S= [K] (H(M) + XY) | mad g = 18 (7 + 7.4) mad 17 => (4, 1) Venty: V=[(gwy y 2) mad p] mad g w=(5') nod g = (72 66 mod 103 mod 17 = 1 mad 11 = (= 12 mad 19 MI= TH(M) w | mad g/ = 4 = 7 = 7. / mod M = 7 Verified! Wz= 7 w mad g = 4.1 mod 17 = 4

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=11 = 1 × // contendate the Jain (X) has the period $S = \frac{di}{ds}$ and select the (860 mad 77 = 1) most frequently occurring dehuminator mol And the 1cm (2,4,5,6) gcd (42,47) = 7 gcd (44,11) =