列印成品

2024年5月10日　　下午 03:50

Introduction to Cryptography, Spring 2024

Homework 5

Due: 5/21/2024 (Tuesday)

Notes:

(1) For Part A, submit a "hardcopy" right after the class on the due day.

(2) TAs will run plagiarism check on your submitted programs. Write your own code and do not copy from others or anywhere.

Part A: Written Problems

1. Consider the elliptic curve $E_{17}(1,2)$. Compute the following values.
   a. All points on the curve.
   b. – (3, 10)
   c. (1, 2)+(3, 10)
   d. 2(3, 10)
2. Consider to use the above cure for EC-ElGamal encryption. Let G=(3,10). Assume that the private key is $n_A = 5$.
   a. What is the public key?
   b. What is the ciphertext of message $P_m = (1, 15)$ when k=4?
   c. Decrypt the above ciphertext and verify its correctness.
3. Compute the signature of M = "Welcome!" using the specified methods. The hash value of a string x is the last 4 bits of of SHA256(*x*). If a number is put into the hash function, convert it to a string by its ASCII code, such as, 25 → 0x3035.
   a. RSA: private key (d, n) = (247, 323)
   b. ElGamal: private key (q, α, X_A) = (103, 11, 37)
   c. Schnorr: private key (p, q, a, s) = (103, 17, 72, 10)
   d. DSA: private key (p, q, g, *x*) = (103, 17, 72, 7)
4. Compute the public keys of the above problem and verify correctness of the signatures.
5. Consider to use RSA with a fixed key for constructing a hash function RSAH as follows. Let message M be partitioned into blocks $B_1B_2\ldots B_n$, where each block is significantly smaller than the modulus of RSA key. The function RSAH is: $RSAH(B_1)=RSA(B_1)$ and $RSAH(B_1B_2\ldots B_n)=RSA(RSAH(B_1B_2\ldots B_{n-1})\oplus B_n)$ for $n\geq 2$. Show that RSAH is not weak collision-resistant.

Part 2: Programming Problem

This programming problem is to simulate the bitcoin mining and build a blockchain. Note that this is not the real bitcoin mining. It only verifies the difficulty of finding hash values with many leading zeros. Use Crypto++ for computing sha256.

1. Consider the following example:
   a. Initial message: "Bitcoin", where its hash value is:
      `B4056DF6691F8DC72E56302DDAD345D65FEAD3EAD9299609A826E2344EB63AA4`
   b. `Build the blockchain as follows:`

# of leading zeros	Preimage = Previous hash (in Hex)+ Nonce (32 bits, in Hex)	Hash value (in Hex), with the specified leading zeros (in Hex)
0	**B4056DF6691F8DC72E56302DDAD345D6 5FEAD3EAD9299609A826E2344EB63AA4** **00000000**	**2767667C2AF3BE01EFAC4FB387EC27C1 0B9D3BEE9C5D48CFF4CFB9F523560B24**
1	**2767667C2AF3BE01EFAC4FB387EC27C1 0B9D3BEE9C5D48CFF4CFB9F523560B24** **0000000A**	**0DE32E85C2AC9D96659D42C8A3EA3D2C 05FDE384B468E6EFE062B6E21288CBCA**
2	?	?
3	?	?
…	?	?

   c. `The blockchain is specified as:`

```
0
B4056DF6691F8DC72E56302DDAD345D65FEAD3EAD9299609A826E2344EB63AA4
00000000
2767667C2AF3BE01EFAC4FB387EC27C10B9D3BEE9C5D48CFF4CFB9F523560B24
1
2767667C2AF3BE01EFAC4FB387EC27C10B9D3BEE9C5D48CFF4CFB9F523560B24
0000000A
0DE32E85C2AC9D96659D42C8A3EA3D2C05FDE384B468E6EFE062B6E21288CBCA
...
```

2. **Your program**
   a) Initial message: your ID in ASCII.
   b) Output: a blockchain like 1.(c), to file out.txt
   c) A block contains 4 separate lines. For example, the above has two blocks.
   d) Your program will be run for verifying your output.
3. **Submission**
   a. **due: 5:00pm, 5/21/2024 (Tuesday)**
   b. **submit two files "blockchain.cpp" and "out.txt" to E3.**
4. Grading: the more leading zeros your hash values have, the higher your grade is.
5. There is no on-site test for this programming problem.

Solutions

1. (a) $y^2 = x^3 + x + 2 \pmod{17}$

points: $(0,6), (0,11), (1,2), (1,15)$
$(3,7), (3,10), (4,6), (4,11)$
$(5,8), (5,9), (9,3), (9,14)$
$(10,3), (10,14), (11,1), (11,16), (12,5), (12,12)$
$(13,6), (13,11), (15,3), (15,14)$
$(16,0)$

(b) $-(3,10) = (3,-10) = (3,7)$

(c) $(1,2) + (3,10)$:

$$\lambda = \frac{10-2}{3-1} \bmod 17 = 4$$

$$x_R = 4^2 - 1 - 3 \pmod{17} = 12$$

$$y_R = 4(1-12) - 2 \pmod{17} = 5$$

$$\Rightarrow (1,2) + (3,10) = (12,5)$$

(d) $2(3,10)$:

$$\lambda = \frac{3 \cdot 3^2 + 1}{2 \cdot 10} \pmod{17} = \frac{7}{5} \bmod 17$$

$$= 7 \times 7 \bmod 17$$

$$= 15$$

$$x_R = 15^2 - 3 - 3 \pmod{17} = 15$$

$$y_R = 15(3-15) - 10 \pmod{17} = 14$$

$$\Rightarrow 2(3,10) = (15,14)$$

2. (a) $PK: 5(3,10) = 4(3,10) + (3,10)$

$$= 2(15,14) + (3,10)$$

$= (10, 11)$

(b) $C = [4(3,10),\ 4(0,11) + (1,15)]$

$= [(12,5),\ (12,12) + (1,15)] = [(12,5), (0,11)]$

(c) $P = (0,11) - 5(12,5)$

$= (0,11) - (12,12)$

$= (0,11) + (12,5)$

$= (1,15) = P_m$

3. (a) $c = H(\text{Welcome!})^{247} \bmod 323$

$= 14^{247} \bmod 323$

$= 40$

(b) let $k = 5$

$C = (2^5 \bmod 103,\ k^{-1}(m - X_A s_1) \bmod 102)$

$= (62,\ 5^{-1}(14 - 37) \cdot 62) \bmod 102)$

$= (62, 54)$

(c) let $r = 5$

$x = 72^5 \bmod 103 = 8$

$e = H(M118) = 2$

$y = (5 + 10 \cdot 2) \bmod 17 = 8$

signature $= (2, 8)$

(d) let $k = 5$

$r = 72^5 \bmod 103 \bmod 17 = 8$

$s = 5^{-1}(14 + 7 \cdot 8) \bmod 17 = 14$

signature $= (8, 14) = (r, s)$

4. (a) $323 = 17 \times 19$

$\varphi(n) = 16 \times 18 = 288$

$e = d^{-1} \bmod 288 = 7$

verify: $C^7 \bmod 323$

$= 40^7 \bmod 323$

$= 14 = H(M)$

(b) $Y_A = \alpha^{X_A} \bmod q$

$= 11^{37} \bmod 103$

$= 67$

verify: $Y_A^{s1} s_1^{s2} \bmod q$

$= 67^{62} 62^{54} \bmod 103 = 83$

$\alpha^m = 11^{14} \bmod 103 = 83$

(c) $v = a^{-s} \bmod 103$

$= 72^{-10} \bmod 103$

$= 72^{92} \bmod 103$

$= 66$

verify: $x' = 72^8 \, 66^2 \bmod 103 = 8$

$H(M \| x') = H(M \| 8) = 2$

(d) $y = 72^7 \bmod 103$

$= 66$

verify: $w = 14^{-1} \bmod 17 = 11$

$u_1 = 14 \cdot 11 \bmod 17 = 1$

$u_2 = 8 \cdot 11 \bmod 17 = 3$

$v = 72^1 \, 66^3 \bmod 103 \bmod 17$

$v = 72^1 \cdot 66^3 \bmod 103 \bmod 17$

$= 8 = r'$

5. For given $M_1 = B_1 B_2 \cdots B_n$, we can find $M_2 = B_1' B_2' \cdots B_{n-1}' B_n'$ such that $B_1', B_2', \cdots, B_{n-1}'$ are random strings of the same lengths of $B_1, B_2 \cdots, B_{n-1}$, respectively, and $B_n' = RSAH(B_1 \cdots B_{n-1}) \oplus RSAH(B_1' B_2' \cdots B_{n-1}') \oplus B_n$.

We can see that

$RSAH(B_1' B_2' \cdots B_n')$

$= RSA(RSAH(B_1' B_2' \cdots B_{n-1}') \oplus B_n')$

$= RSA(RSAH(B_1 B_2 \cdots B_{n-1}) \oplus B_n)$

$= RSAH(B_1 B_2 B_3 \cdots B_n)$

Thus, $B_1 B_2 \cdots B_n$ and $B_1' B_2' \cdots B_n'$ have a collision hash.

RSAH is not weak collision-resistant.