Homework 1 solutions

---

1 . Use Euler's theorem to find the following results:

a). 17^{-1}mod 480

$\varphi(480) = \varphi(2^5) * \varphi(3) * \varphi(5)$
$= (2^5-2^4) * 2 * 4$
$= (32-16) * 8$
$= 128$

17^{-1}mod 480 = $17^{\varphi(480)-1} = 17^{127}$ mod 480 = 113

b). 11^{192002}mod 2800

$\varphi(2800) = \varphi(2^4) * \varphi(5^2) * \varphi(7)$
$= (2^4-2^3) * (5^2-5) * 6$
$= (16-8) * (25-5) *$
$= 8 * 20 * 6$
$= 960$

$11^{200* 960 + 2}$ mod 2800 = 11^2 mod 2800 = 121

---

2. Calculate the followings:

a) $\varphi(228)$

$\varphi(228) = \varphi(2^2) * \varphi(3) * \varphi(19)$
$= (2^2 – 2^1) * 2 * 18$
$= (4 – 2) * 36$
$= 2 * 36$
$= 72$

b) $\varphi(445)$

$\varphi(445) = \varphi(5) * \varphi(89)$
$= 4 * 88$
$= 352$

c) $\varphi(302)$

$\varphi(302) = \varphi(2) * \varphi(151)$
$= 1 * 150$
$= 150$

d) the order of the group <Z194*, x>

$\varphi(194) = \varphi(2) * \varphi(97) = 96$

---

3. RSA. Alice wants to generate a pair of RSA public and private keys. She starts by selecting two primes p = 11 and q = 23. She selects e = 19. Suppose Bob's key pair is PUB=(17, 551), PRB=(89,551). (Note: PU means public key, PR means private key). Alice and Bob have already told each other's public key.

a) What are Alice's public key and private key?

$n = 11*23 = 253$

$\varphi(253) = (11-1) \times (23-1) = 10 * 22 = 220$

$\varphi(220) = \varphi(2^2 \times 5 \times 11) = 110$

$d = 19^{-1} \bmod 220 = 19^{\varphi(220) - 1} \bmod 220 = 19^{110-1} \bmod 220 = 19^{109} \bmod 220 = 139$

Alice's public key: (19, 253)

Alice's private key: (139, 253)

b) Bob wants to send Alice a message M=25 which only Alice can read. What's the ciphertext C? After Alice receives C, how does she decrypt C to get M?

M should be encrypted with Alice's public key

$C = M^e \bmod n = 25^{19} \bmod 253 = 26$

Alice decrpts C with her private key

$M = C^d \bmod n = 26^{139} \bmod 253 = 25$

c) Bob sends the same M=25 again to Alice. Bob wants to let Alice know that M is from him. How does he sign M? How does Alice verify the signature?

Bob signs M with his private key

$S = M^d \bmod n = 25^{89} \bmod 551 = 339$

Bob sends 25||339 to Alice

Alice verifies S with Bob's public key

$M' = S^e \bmod n = 518^{17} \bmod 551 = 25$

M = M', M is accepted.

d) Alice wants to send Bob the message M = 25 to Bob. Now, she doesn't care about others reading M. She only wants to let Bob know that M is sent from her not from anyone else. How does she sign the M? How does Bob verify the signature?

Alice signs M with her private key

$S = M^d \bmod n = 25^{139} \bmod 253 = 59$

Alice sends 25||59to Bob

Bob verifies S with Alice's public key

$M' = S^e \bmod n = 59^{19} \bmod 253 = 25$

M = M', M is accepted.

---

4. Using the irreducible polynomial $f(x) = x^5+x^2+1$ to

a) generate the elements of the field $GF(2^5)$

From the irreducible polynomial, we get:

$x^5 = -x^2-1$

Since addition and subtraction are the same operation,

$x^5 = x^2+1$

$0 = 0$	$= 0$	$= 0$	à	0 =(00000)
$g^0 = g^0$	$= g^0$	$= g^0$	à	g^0 =(00001)
$g^1 = g^1$	$= g^1$	$= g^1$	à	g^1 = (00010)
$g^2 = g^2$	$= g^2$	$= g^2$	à	g^2 = (00100)
$g^3 = g^3$	$= g^3$	$= g^3$	à	g^3 = (01000)
$g^4 = g^4$	$= g^4$	$= g^4$	à	g^4 = (10000)
$g^5 = g^5$	$= g^5$	$= g^2 +1$	à	g^5 = (00101)
$g^6 = g(g^5) = g(g^2+1)$		$= g^3 +g$	à	g^6 = (01010)
$g^7 = g(g^6) = g(g^3 +g)$		$= g^4+ g^2$	à	g^7 = (10100)
$g^8 = g(g^7) = g(g^4 +g^2)$		$= g^5+ g^3 = g^3+ g^2+1$	à	g^8 = (01101)
$g^9 = g(g^8) = g(g^3 +g^2+1)$		$= g^4+ g^3+g$	à	g^8 = (11010)
$g^{10} = g(g^9)$	$= g(g^4 + g^3 + g)$	$= g^5 + g^4 + g^2 = g^4 + 1$	à	g^{10} = (10001)
$g^{11} = g(g^{10})$	$= g(g^4 + 1)$	$= g^5 + g = g^2 + g + 1$	à	g^{11} = (00111)
$g^{12} = g(g^{11})$	$= g(g^2 + g + 1)$	$= g^3 + g^2 + g$	à	g^{12} = (01110)
$g^{13} = g(g^{12})$	$= g(g^3 + g^2 + g)$	$= g^4 + g^3 + g^2$	à	g^{13} = (11100)
$g^{14} = g(g^{13})$	$= g(g^4 + g^3 + g^2)$	$= g^5 + g^4 + g^3 = g^4 + g^3 + g^2 + 1$	à	g^{14} = (11101)

$g^{15} = g(g^{14})$ $= g(g^4 + g^3 + g^2 + 1)$ $= g^5 + g^4 + g^3 + g = g^4 + g^3 + g^2 + g + 1$ à $g^{15} = (11111)$

$g^{16} = g(g^{15})$ $= g(g^4 + g^3 + g^2 + g + 1)$ $= g^5 + g^4 + g^3 + g^2 + g = g^4 + g^3 + g + 1$ à $g^{16} = (11011)$

$g^{17} = g(g^{16})$ $= g(g^4 + g^3 + g + 1)$ $= g^5 + g^4 + g^2 + g = g^4 + g + 1$ à $g^{17} =$ (10011)

$g^{18} = g(g^{17})$ $= g(g^4 + g + 1)$ $= g^5 + g^2 + g = g + 1$ à $g^{18} = (00011)$

$g^{19} = g(g^{18})$ $= g(g + 1)$ $= g^2 + g$ à $g^{19} = (00110)$

$g^{20} = g(g^{19})$ $= g(g^2 + g)$ $= g^3 + g^2$ à $g^{20} = (01100)$

$g^{21} = g(g^{20})$ $= g(g^3 + g^2)$ $= g^4 + g^3$ à $g^{21} = (11000)$

$g^{22} = g(g^{21})$ $= g(g^4 + g^3)$ $= g^5 + g^4 = g^4 + g^2 + 1$ à $g^{22} =$ (10101)

$g^{23} = g(g^{22})$ $= g(g^4 + g^2 + 1)$ $= g^5 + g^3 + g = g^3 + g^2 + g + 1$ à $g^{23} =$ (01111)

$g^{24} = g(g^{23})$ $= g(g^3 + g^2 + g + 1)$ $= g^4 + g^3 + g^2 + g$ à $g^{24} = (11110)$

$g^{25} = g(g^{24})$ $= g(g^4 + g^3 + g^2 + g)$ $= g^5 + g^4 + g^3 + g^2 = g^4 + g^3 + 1$ à $g^{25} =$ (11001)

$g^{26} = g(g^{25})$ $= g(g^4 + g^3 + 1)$ $= g^5 + g^4 + g = g^4 + g^2 + g + 1$ à $g^{26} = (10111)$

$g^{27} = g(g^{26})$ $= g(g^4 + g^2 + g + 1)$ $= g^5 + g^3 + g^2 + g = g^3 + g + 1$ à $g^{27} = (01011)$

$g^{28} = g(g^{27})$ $= g(g^3 + g + 1)$ $= g^4 + g^2 + g$ à $g^{28} =$ (10110)

$g^{29} = g(g^{28})$ $= g(g^4 + g^2 + g)$ $= g^5 + g^3 + g^2 = g^3 + 1$ à $g^{29} =$ (01001)

$g^{30} = g(g^{29})$ $= g(g^3 + 1)$ $= g^4 + g$ à $g^{30} = (10010)$

b) based on the results of a), calculate

b.1) $(x^4 + x^2 + 1)^{-1}$ MOD $(x^5 + x^2 + 1)$

$x^4 + x^2 + 1 = g^{22}$

$(g^{22})^{-1} = g_{-}^{22 \text{ mod } 31} = g_{-}^{22 + 31} = g^9 = g^4 + g^3 + g$

$(x^4 + x^3 + x)$ MOD $(x^5 + x^2 + 1) = x^4 + x^3 + x$

b.2) $(x^4 - x^3 + 1) * (x^3 + x^2 + x + 1)$

$(x^4 + x^3 + 1) * (x^3 + x^2 + x + 1) = (g^{25}) * (g^{23}) = g^{48 \text{ mod } 31} = g^{17} = x^4 + x + 1$

b.3) $(x^4 - x^2 + 1) / (x^3 + x^2 + x + 1)$

$(x^4 + x^2 + 1) / (x^3 + x^2 + x + 1) = (g^{22}) / (g^{23}) = g^{-1 \bmod 31} = g^{-1+31} = g^{30} = x^4 + x$

---

5. ElGamal signature scheme. Let p=881, e1 = 3, d=61. find e2. Choose r (it's up to you to decide the value of r). Find the values of s1 and s2 if M=400. Verify the signature.

a) Generate the signature

$e2 = e1^d \bmod p = 3^{61} \bmod 881 = 589$

M = 400, suppose r is 7

$S1 = e1^r \bmod p = 3^7 \bmod 881 = 425$

$S2 = (M - d*S1)r^{-1} \bmod (p-1)$

$= (400 - 61*425) * 7^{-1} \bmod (880)$

$(400 - 61*425) \bmod 880 = -25525 \bmod 880 = 875$

$7^{-1} \bmod 880 = 7^{ø(880)-1} = 7^{ø(16*5*11)-1} = 7^{320-1} \bmod 880 = 503$

So, S2 = (875 x 503) mod 880 = 125

The sender sends M = 400, S1 = 425, S2 = 125 to the receiver.

b) To verify the signature, the receiver calculates:

$V1 = e1^M \bmod p = 3^{400} \bmod 881 = 186$

$V2 = e2^{S1} * S1^{S2} \bmod p$

$= 589^{425} * 425^{125} \bmod 881$

$= 267 * 852 \bmod 881 = 186$

V1 = V2, the signature is accepted.

---

6. DSS scheme. Let p = 743, q = 53, d = 52 and e0=5. Find values of e1 and e2. Choose r = 17. Find the values of S1 and S2 if h(M) = 120. Verify the signature.

Find values of e1 and e2.
Choose r = 13. Find the values of S1 and S2 if h(M) = 120.
Verify the signature

$e_1 = e_0^{(p-1)/q} \bmod p$

$= 5^{742/53} \bmod 743$

$= 5^{14} \bmod 743$

$= 212$

$e_2 = e_1^d \bmod p$

$= 212^{52} \bmod 743$
$= 368$

$S_1 = (e_1{}^r \bmod p) \bmod q$
$= (212^{17} \bmod 743) \bmod 53$
$= 147 \bmod 53$
$= 41$

$S_2 = (h(M) + dS_1)\, r^{-1} \bmod q$
$= ((120 + 52(41))\, 17^{-1}) \bmod 53$
$= (120 + 2132)\, 17^{\Phi(53) - 1} \bmod 53$
$= (2252)17^{51} \bmod 53$
$= (2252 \bmod 53) \times (17^{51} \bmod 53) \bmod 53$
$= 26 \times 25 \bmod 53$
$= 14$

So the signature is $(S_1, S_2) = (41, 14)$

To verify the signature
$V = (e_1{}^{h(M)S2\text{^}-1}\, e_2{}^{S1S2\text{^}-1} \bmod 743) \bmod 53$
$V = (212^{14(S2\text{^}-1)}\, 368^{14(S2\text{^}-1)} \bmod 743) \bmod 53$
$S_2{}^{-1} = 14^{-1} \bmod 53$
$= 14^{\Phi(53) - 1} \bmod 53$
$= 14^{51} \bmod 53 = \mathbf{19}$

$V = (212^{120(19)}\, 368^{41(19)} \bmod 743) \bmod 53$
$= (212^{(2280 \bmod 53)} \times 368^{(779 \bmod 53)} \bmod 743) \bmod 53$
$= (212 \times 368^{37} \bmod 743) \bmod 53$
$= (212 \times 600 \bmod 743) \bmod 53$
$= 147 \bmod 53$
$= 41$

$V = S_1 = 41$, the signature is verified.

---

7. Users A and B use the Diffie-Hellman key exchange technique with a common prime p=199 and a primitive root g = 6

a) If user A has private key x = 33, what is A's public key R1?

$R1 = g^x \bmod p = 6^{33} \bmod 199 = 93$

b) If user B has private key y = 49, what's B's public key R2?

$R2 = g^y \bmod p = 6^{49} \bmod 199 = 113$

c) How does A and B calculate the shared secret key?

A: $K_{AB} = R2^x \bmod p = 113^{33} \bmod 199 = 93$

B: $K_{AB} = R1^y \bmod p = 93^{49} \bmod 199 = 93$

d) If user C just joined the group and his private key is 18. What's the security key between A and C? What's the security key between B and C?

C's public key: $R3 = 6^{18} \bmod 199 = 63$

A: $K_{AC} = R3^x \bmod 199 = 63^{33} \bmod 199 = 1$

C: $K_{AC} = R1^z \bmod 199 = 93^{18} \bmod 199 = 1$

B: $K_{BC} = R3^y \bmod 199 = 63^{49} \bmod 199 = 61$

C: $K_{BC} = R2^z \bmod 199 = 113^{18} \bmod 199 = 61$

---

8. In a PGP community, the following trust relationship exits:

a) Alice fully trust John
b) Alice partially trust Cathy and Bob.
c) Alice doesn't trust Jason.

For each of the following successive events, give the content of Alice's public keying table. Note, it's up to you to choose the public key and the key ID of each person. You can ignore the timestamp field. The initial table is:

1) Alice called John to get John's public key and add it to the table.

User ID	Key ID	Public Key	Producer trust	Certificate	Cert. trust	Key legit.
Alice	Alice1	111111	F			F
John	John	222222	F			F

2) Alice got Cathy's certificate issued by Bob and add her to the table

User ID	Key ID	Public Key	Producer trust	Certificate	Cert. trust	Key legit.
Alice	Alice1	111111	F			F
John	John	222222	F			P
Cathy	Cathy	333333	P	Bob's	P	P

3) Alice received Bob's certificate issued by Cathy and add him to the table

User ID	Key ID	Public Key	Producer trust	Certificate	Cert. trust	Key legit.
Alice	Alice1	111111	F			F
John	John	222222	F			F
Cathy	Cathy	333333	P	Bob's	P	P
Bob	Bob	4444444	P	Cathy's	P	P

4) Alice received Bob's certificate issued by John and add him to the table

User ID	Key ID	Public Key	Producer trust	Certificate	Cert. trust	Key legit.
Alice	Alice1	111111	F			F
John	John	222222	F			F
Cathy	Cathy	333333	P	Bob's	P	P
Bob	Bob	4444444	P	Cathy's John's	P F	F

5) Alice received Jason's certificate issued by Cathy.

User ID	Key ID	Public Key	Producer trust	Certificate	Cert. trust	Key legit.
Alice	Alice1	111111	F			F
John	John	222222	F			F
Cathy	Cathy	333333	P	Bob's	P	P
Bob	Bob	4444444	P	Cathy's John's	P F	F
Jason	Jason	555555	N	Cathy's	P	P

6) Alice received Jason's certificate issued by Bob.

User	Key ID	Public Key	Producer trust	Certificate	Cert. trust	Key legit.

ID						
Alice	Alice1	111111	F			F
John	John	222222	F			F
Cathy	Cathy	333333	P	Bob's	P	P
Bob	Bob	4444444	P	Cathy's John's	P F	F
Jason	Jason	555555	N	Cathy's Bob's	P P	F

9. SET. Suppose PI = 71, OI =94. The hash function is h(x) = (x+11) mod 291. The customer's key pair is:
public key{17, 377}, private key{257, 377}. Concatenation works like this: 23||45 = 2345. Assume that both the merchant and the bank know the public key of the customer. The signature algorithm is RSA.
1) What's the dual signature created by the customer? Describe in detail how the customer create it.

H(PI) = (71 + 11) mod 291 = 82 mod 291 = 82

H(OI) = (94 + 11) mod 291 = 105 mod 291 = 105

H(H(PI) || H(OI)) = H(82 || 105) = (82105 + 11) mod 291 = 82116 mod 291 = 54

E(PRc, [H(H(PI) || H(OI))]) = 54^{257} mod 377 = 136

DS = 136

2) What information does the merchant need to know to verify the dual signature and how to verify it?

The merchant needs to know OI, PIMD, DS

H[(PIMD) || H(OI)]

H(OI) = (94 + 11) mod 291 = 105 mod 291 = 105

PIMD = 82

H[(PIMD) || H(OI)] = H(82 || 105) = (82105 + 11) mod 291 = 82116 mod 291 = 54

D(PUC, DS)

D(PUC, DS) = 136^{17} mod 377 = 54

POMD = D(PUC, DS)

The dual signature is verified.

3) What information does the bank need to know to verify the dual signature and how to verify it?

H[H(PI) || OIMD]

H(PI) = (71 + 11) mod 291 = 82 mod 291 = 82

OIMD = 105

H[H(PI) || OIMD] = H(82 || 105) = (82105 + 11) mod 291 = 82116 mod 291 = 54

D(PUC, DS)

D(PUC, DS) = 136^{17} mod 377 = 54

POMD = D(PUC, DS)

The dual signature is verified.

10(AONDS). Alice has the following 4 12-bit secrets for sale:

S1=1091, S2=1472, S3=1461 S4=1168

Bob wants to buy S2 and Carol wants to buy S4.

The key pair for Bob is n=7387, e=5145, d=777. The key pair for Carol is n=2747,e=1421,d=2261. She tells Bob and Carol each their public key

Please describe step by step how Bob and Carol buy the secrets they want without letting Alice know which secrets they are buying.

* Bob generates 4 12-bit random numbers and sends the numbers to Carol

B1 = 743 = 001011100111

B2 = 1988 = 011111000100

B3 = 2001 = 011111010001

B4 = 2~~942 = 101101111110 1942~~ = 0111 1001 0110

* Carol generates 4 12-bit random numbers and sends the numbers to Bob

C1 = 1708 = 011010101100

C2 = 772 = 001100000011

C3 = 1969 = 011110110001

C4 = 3112 = 110000101000

* Bob wants to buy S2, so he encrypts C2=772 with his public key

772^5145 mod 7387 = 3768

Now, 772 = 0011 0000 0100

3768 = 1110 1011 1000

So, the FBI of the two numbers is [0,1,6,9].

Bob sends [2,3,4,5,7,8,10,11] to Carol

Carol wants to buy S4, so he encrypts B4=~~2942~~ 1942 with her public key

1942^1421 mod 2747 = 2076

Now, 1942 = 0111 1001 0110

2076 = 1000 0001 1100

So, the FBI of the two numbers is [0,2,4,5,6].

Carol sends [1,3,7,8,9,10,11] to Bob

* Bob takes B1, B2, B3, B4 and replaces every bit whose index is in the set [1,3,7,8,9,10,11] with its complement.

B1'= 1101 0110 1101 (0010 1110 0111) = 3437

B2'= 1000 0100 1110 (0111 1100 0100) = 2126

B3'= 1000 0101 1011 (0111 1101 0001) = 2139

B4'= 1000 0001 1100 (0111 1001 0110) = 2076

Bob sends B1', B2', B3' and B4' to Alice

Carol takes C1, C2, C3, C4 and replaces every bit whose index is in the set

[2,3,4,5,7,8,10,11] with its complement.

C1' = 1011 0001 0000 (0110 1010 1100) = 2832

C2' = 1110 1011 1000 (0011 0000 0100) = 3768

C3' = 1010 0000 1101 (0111 1011 0001) = 2573

C4' = 0001 1001 0100 (1100 0010 1000) = 404

Carol sends C1', C2', C3' and C4' to Alice

* Alice decrypts all Ci' with Bob's private key (777, 7387) and XORs the results with Si.

i=1 2832^777 mod 7387 = 1538; 1538 **Å** 1091 = 757
i=2 3768^777 mod 7387 = 772; 772 **Å** 1472 = 1732
i=3 2573^777 mod 7387 = 4316; 4316 **Å** 1461=5481
i=4 404^777 mod 7387 = 6415; 6415 **Å** 1168 = 7583

She sends (677,1732,5481,7583) to Bob

Alice decrypts all Bi' with Carol's private key (2261, 2747) and XORs the results with Si.

i=1 3437^2261 mod 2747 =1770; 1770**Å** 1091= 681
i=2 2126^2261 mod 2747 = 1400; 1400**Å** 1472 = 184
i=3 2139^2261 mod 2747 = 1756; 1756**Å** 1461= 873
i=4 2076^2261 mod 2747 = 1942 1942**Å** 1168 = 774

She sends (1676, 1877, 4075, 4078) to Carol.

Bob computes S2 by XORing C2 and the 2nd number he received from Alice
772 **Å** 1732 = 1472

Carol computes S4 by XORing B4 and the 4th number he received from Alice
1942 **Å** 774= 1168