Homework 2 solution

---

1. Use CRT to solve the following set of equations:

$$x = 5 \bmod 17$$

$$x = 9 \bmod 21$$

$$x = 7 \bmod 23$$

1) $M = 17 * 21 * 23 = 8211$
2) $M1 = 21*23 = 483$, $M2 = 17*23 = 391$, $M3 = 17 * 21 = 357$
3) $M1^{-1} = 483^{15} \bmod 17 = 5$, $M2^{-1} = 391^{11} \bmod 21 = 13$, $M3^{-1} = 357^{21} \bmod 23 = 2$
4) $x = (5 * 483 * 5 + 9 * 391 * 13 + 7 * 357 * 2) \bmod 8211 = 5343$

---

2. Using quadratic residues, solve the following congruences:

a. $x^2 \equiv 5 \bmod 11$

$a^{(p-1)/2} \bmod p = 5^{(11-1)/2} \bmod 11$
$= 5^5 \bmod 11$
$= 1 \bmod 11$
so 5 is a QR and the equation has two solutions

$x_1 = a^{(p+1)/4} \bmod p$
$= 5^{(11+1)/4} \bmod 11$
$= 5^3 \bmod 11$
$= 4 \bmod 11$

$x_2 = -a^{(p+1)/4} \bmod p$

$= -5^{(11 + 1)/4} =$
$= -125 \bmod 11$
$= 7 \bmod 11$

b. $x^2 \equiv 4 \bmod 133$

$133 = 7 * 19$

The equation can be split into 2 equations:
$x^2 \equiv 4 \bmod 7$ and $x^2 \equiv 4 \bmod 19$

The 1st equation has 2 solutions: $x = 4^{(7+1)/4} \bmod 7 = 2 \bmod 7$,
$x = -4^{(7+1)/4} \bmod 7 = 5 \bmod 7$
The 2nd equation has 2 solutions: $x = 4^{(19+1)/4} \bmod 7 = 2 \bmod 19$
$x = -4^{(19+1)/4} \bmod 7 = -2 \bmod 19 = 17 \bmod 19$

set 1: $x = 2 \bmod 7$ $x = 2 \bmod 19$
use CRT to solve the set of equations

$M = 7 * 19 = 133$
$M1 = 133/7 = 19$ $M1^{-1} \bmod 7 = 19^{-1} \bmod 7 = 19^5 \bmod 7 = 3 \bmod 7$

$M2 = 133/19 = 7$ $M2^{-1} \bmod 19 = 7^{-1} \bmod 19 = 7^{17} \bmod 19 = 11 \bmod 19$

$x = (2*19*3 + 17*7*11) \bmod 133 = 114 + 1309 = 93 \bmod 133$

set 2: $x = 5 \bmod 7$ $x = 2 \bmod 19$
use CRT to get $x = 2 \bmod 133$

set 3: $x = 2 \bmod 7$ $x = 17 \bmod 19$
use CRT to get $x = -2 \bmod 133$

set 4: $x = 5 \bmod 7$ $x = 17 \bmod 19$
use CRT to get $x = -93 \bmod 133$

---

3. S-AES

a) use the key 1010 0111 0011 1011 to encrypt the data block 0110 1111 0110 1011
0000 0111 0011 1000

b) use the same key 1010 0111 0011 1011 to decrypt the ciphertext 0000 0111 0011 1000

~~0010 0101 0010 0010~~

0110 1111 0110 1011

---

4. Find the results of following, using Fermat's little theorem or Euler's theorem.

a) 16^{52381} mod 19

$\varnothing(19) = 18$

$52381 = 2910*18 + 1$

$16^{52381=18*2910+1}$ mod 19 = 16

b) 78^{-1} mod 115

$\varnothing(115) = \varnothing(5) \times \varnothing(23) = 88$

$78^{-1} = 78^{88-1}$ mod 115 = 87

c) 45^{-1} mod 668

$\varnothing(668) = \varnothing(2^2) \times \varnothing(167) = 2 \times 166 = 332$

45^{-1} mod 668 = 45^{332-1} mod 668 = 193

d) 19^{-1} mod 356

$\varnothing(356) = \varnothing(2^2) \times \varnothing(89) = 2 \times 88 = 176$

19^{-1} mod 356 = 19^{176-1} mod 356 = 75

e) 35^{34994} mod 247

$\varnothing(247) = \varnothing(19) \times \varnothing(13) = 216$

$35^{34994} = 35^{216*162+2} = 35^2$ mod 247 = 237

---

5. RSA

a) In a public key system using RSA, you intercept the ciphertext C=152 sent to Alice whose public key (11,221). What is the plaintext M?

$n = 221 = 13 \times 17$

$\varnothing(n) = 12 \times 16 = 192$

$\varnothing(192) = \varnothing(2^6) \times \varnothing(3) = 32 \times 2 = 64$

$d = e^{-1} \bmod 192 = 11^{-1} \bmod 192 = 11^{64-1} \bmod 192 = 35$

$M = C^d \bmod n = 152^{35} \bmod 221 = 16$

b) Suppose you intercept a message 39 with its signature 96 signed by Bob whose public key is (13, 209). You want to change the message 39 to 49. How do you create a valid signature for 49?

$n = 209 = 11 \times 19$

$ø(n) = 10 \times 18 = 180$

$ø(180) = ø(2^2) \times ø(3^2) \times ø(5) = 2 \times 6 \times 4 = 48$

$d = e^{-1} \bmod 180 = 13^{-1} \bmod 180 = 13^{48-1} \bmod 180 = 97$

$S = M^d \bmod n = 49^{97} \bmod 209 = 201$

---

6. In ElGammal, given the prime p = 137, e1= 3
a) Choose a d and calculate e2

$d = 6$

$e2 = e1^d \bmod p = 3^6 \bmod 137 = 44$

b) Choose a r (it's up to you to decide the value of r) and encrypt the message "happy"; use 00 to 25 for encoding.

r = 12

C1 = e1^r mod p = 3^7 mod 137 = 18

C2 = (P x e2^r) mod p = (P x 56) mod 137

	P	C2
h	7	(7x56) mod 137= 118

a	0	0
p	15	(15x56) mod 137=18
p	15	(15x56) mod 137=18
y	24	(24x56) mod 137=111

c) Decrypt the ciphertext to obtain the plaintext

C1^(p-1-d) mod p = 18 ^ (137 - 1 - 6) mod p = 115

P = (C2 * C1^(p-1-d)) mod p = (C2 * 115) mod p

C2	P
118	(118x115)mod 137 = 7
18	(18x115)mod 137 = 15
18	(18x115)mod 137 = 15
111	(111x115)mod 137 = 24

---

7. 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).
a)Find the values of s1 and s2 if M=400.

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

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) mod 880 = -25525 mod 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) Verify the signature.

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

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

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

$= 267 * 852 \bmod 881 = 186$

V1 = V2, the signature is accepted.

---

8. In the Diifie-Hellman protocol, g=7, p = 239, x = 18 and y=34.
a) What's the value of the symmetric key?
K = g ^ xy mod p = 7 ^ (18x34) mod 239 = 44

b) What's the value of R1 and R2?

R1 = g^x mod p= 7^18 mod 239 = 170

R2 = g^y mod p = 7^34 mod 239 = 24

9.DSS scheme. Let p = 743, q = 53, d = 56 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

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

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

$= 5^{14} \bmod 743$

$= 212$

$e_2 = e_1^{d} \bmod p$

$= 212^{56} \bmod 743$

$= 639$

$S_1 = (e_1^{r} \bmod p) \bmod q$

$= (212^{17} \bmod 743) \bmod 53$

$= 147 \bmod 53$

$= 41$

$S_2 = (h(M) + dS_1)\, r^{-1} \bmod q$

$= ((120 + 56(41))\, 17^{-1}) \bmod 53$

$= (120 + 2296)\, 17^{\Phi(53) - 1} \bmod 53$

$= (2252)17^{51} \bmod 53$

$= (2416 \bmod 53) \times (17^{51} \bmod 53) \bmod 53$

$= 31 \times 25 \bmod 53$

= 33

So the signature is $(S_1, S_2) = (41, 33)$

To verify the signature

$V = (e_1^{h(M)S2^\wedge-1}\ e_2^{S1S2^\wedge-1} \bmod 743) \bmod 53$

$S_2^{-1} = 33^{-1} \bmod 53$

$= 33^{\Phi(53)-1} \bmod 53$

$= 33^{51} \bmod 53 = \mathbf{45}$

$V = (212^{120 \text{ x } 45)}\ 639^{41\text{x}45} \bmod 743) \bmod 53$

$= (212^{(5400 \bmod 53)} \text{ x } 639^{(1845 \bmod 53)} \bmod 743) \bmod 53$

$= (212^{47} \text{ x } 639^{43} \bmod 743) \bmod 53$

$= (271 \text{ x } 675 \bmod 743) \bmod 53$

$= 147 \bmod 53$

$= 41$

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