Homework 3 solutions

Total points: 10

1. [illegible] AES (Show [illegible] ults in [illegible])

a) [illegible] te the three [illegible] ys bas[illegible] 1001 [illegible]

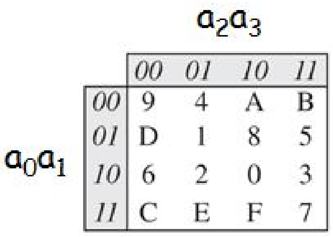
b) Encrypt the data block 0101 0110 1101 0011

c) Decrypt the ciphertext block 0010 1111 0001 1001

$$= \begin{bmatrix} 1101 \\ 0010 + g^{15} \end{bmatrix} = \begin{bmatrix} 1101 \\ 0011 \end{bmatrix} = \begin{bmatrix} D \\ 3 \end{bmatrix}$$

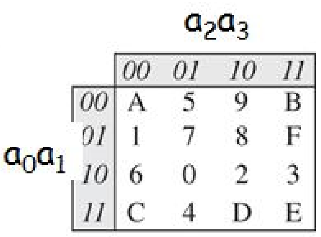
a) Key = 1001 1111 0100 0010 = 9F42

Round	Values of t's	1^{st} word in the round	2^{nd} word in the round	Round key
0		w0=9F	w1=42	k0=9F42
1	t2=2D	W2=2D ⊕9F=B2	w3=B2 ⊕ 42 = F0	k1=B2F0
2	t4=A7	W4=A7 ⊕B2 = 15	W5=15⊕F0 = E5	k2=15E5



a_0a_1 \ a_2a_3	00	01	10	11
00	9	4	A	B
01	D	1	8	5
10	6	2	0	3
11	C	E	F	7

SubNibbles table



a_0a_1 \ a_2a_3	00	01	10	11
00	A	5	9	B
01	1	7	8	F
10	6	0	2	3
11	C	4	D	E

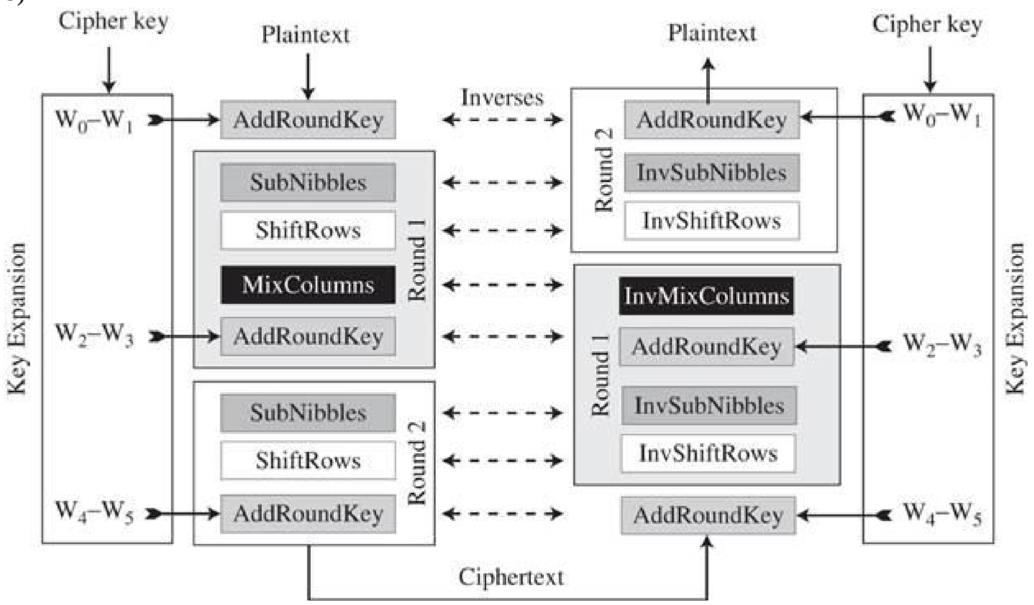
InvSubNibbles table

t2 = RotWord(42)=24àSubWord(24)= ADàt$_2$ = AD ⊕ RC[1] = AD ⊕ 80 = 2D

t4 = RotWord(F0)= 0F àSubWord(0F)=97 àt$_4$ = 97 ⊕ RC[2] = 97 ⊕ 30 = A7

----

b)



1) Pre-round: AddRoundKey

Data block: 0101 0110 1101 0011 = 56D3

State: $\begin{pmatrix} 5 & D \\ 6 & 3 \end{pmatrix}$

$\begin{pmatrix} 5 & D \\ 6 & 3 \end{pmatrix}$ ARK ---------------------à K0 = 9F42

2) Round 1

SN -------à SR ------à MC -----à ARK -----------à K1=B2F0

$$\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} x \begin{bmatrix} C \\ 4 \end{bmatrix} = \begin{bmatrix} 1xC + 4x4 \\ 4xC + 1*4 \end{bmatrix} = \begin{bmatrix} 1100 + 0100x0100 \\ 0100x1100 + 0100 \end{bmatrix}$$
$$= \begin{bmatrix} 1100 + g^2xg^2 \\ g^2xg^6 + 0110 \end{bmatrix} = \begin{bmatrix} 1100 + g^4 \\ g^8 + 0100 \end{bmatrix} = \begin{bmatrix} 1100 + 0011 \\ 0101 + 0100 \end{bmatrix}$$
$$= \begin{bmatrix} 1111 \\ 0001 \end{bmatrix} = \begin{bmatrix} F \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} x \begin{bmatrix} 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 1x2 + 4x2 \\ 4x2 + 1*2 \end{bmatrix} = \begin{bmatrix} 0010 + 1000 \\ 1000 + 0010 \end{bmatrix}$$
$$= \begin{bmatrix} 1010 \\ 1010 \end{bmatrix} = \begin{bmatrix} A \\ A \end{bmatrix}$$

3) Round 2

SN -------à SR ------à ARK -----à K2=15E5

Ciphertext: C5FE = 1100 0101 1111 1110

----

c) The three round keys are the same, but they should be used in the reverse order.

1) Pre-round: AddRoundKey

Ciphertext block: 0010 1111 0001 1001

$\begin{pmatrix} 2 & 1 \\ F & 9 \end{pmatrix}$

State:

$\begin{pmatrix} 2 & 1 \\ F & 9 \end{pmatrix}$ ARK ---------------------à K2 = 15E5

2) Round 1

The InvSubNibble table should be used

ISR -------à ISN ------à ARK -----à IMC -----------à

K1=B2F0

3) Round 2

ISR -------à ISN ------à ARK -----------à

K0=9F42

The plaintext block is 740D = 0111 0100 0000 1101

2(1pt). Find the results of following, using Fermat's little theorem or Euler's theorem.

a) 15^{116060} mod 53

φ(53) = 52

$15^{116060 \text{ mod } 52}$ = 15^{48} mod 53= 16

b) 49^{-1} mod 416

φ(416) = φ($2^5 13^1$) = ($2^5 – 2^4$)*12 = 192

49^{-1} mod 416 = $49^{\varphi(416)-1}$mod 416 = = 49^{191}mod 416 = 17

c) 101^{-1} mod 598

φ(598) = φ(2*13*23)= 264

101^{-1} mod 598 = $101^{\varphi(598)-1}$mod 598 = = 101^{263}mod 598 = 225

d) $97^{-1} \bmod 1056$

$\varphi(1056) = \varphi(2^5*3*11)= (2^5 - 2^4) *2 *10 = 320$

$97^{-1} \bmod 1056 = 97^{\varphi(1056)-1} \bmod 1056 = 97^{319} \bmod 1056 = 577$

e) $45^{1441251} \bmod 546$

$\varphi(546) = \varphi(2*3*7*13) = 144$

$45^{1441251} \bmod 546 = 45^{1441251 \bmod \varphi(546)} \bmod 546$

$= 45^{99} \bmod 546 = 489$

3(1.5pt). RSA.

1) How to generate a key pair for Alice and Bob respectively? Both primes they pick should be greater than 100 and smaller than ~~1000~~ 300. Click here for a list of primes smaller than 10,000. Two or more students who select the same primes are considered cheating.

	p	q	n	Φ(n)	e	d	Public key	Private key
Alice	131	241	31,571	31,200	101	13,901	(101,31571)	(13901,31571)
Bob	127	151	19,177	18,900	271	10,531	(271,19177)	(10531,19177)

$\varphi(31,200) = \varphi(2\char`^5 * 3 * 5\char`^2 *13) = 16*2*20*12 = 7680$

$101^{-1} = 101^{7680-1} \bmod 31200 = 101^{7679} \bmod 31200 =(101^{1097})^7 \bmod 31200 = 13,901$

$\varphi(18,900) = \varphi(2\char`^2 * 3\char`^3 * 5\char`^2 *13) = 2*18*20*12 = 8640$

$271^{-1} = 271^{8640-1} \bmod 18900 = 271^{8639} \bmod 18900 =(271^{163})^{53} \bmod 18900 = 10,531$

2) Suppose Alice sends plaintext P=113, how does she encrypt and what's the ciphertext C? After Bob receives C, how does he decrypts it to get the plaintext P?

Alice uses Bob's public key to encrypt it:
C = P^e mod n = 113^271 mod 19177 = 10,683

Bob uses his private key to decrypt it:
P = C^d mod n = 10683^10531 mod 19177 = 10683 ^(100*100+531) mod 19177 = 13406*6636 mod 19177 = 113

3) Suppose Bob sends plaintext P=113, how does he encrypt and what's the ciphertext C? After Alice receives C, how does she decrypts it to get the plaintext P?

Bob uses Alice public key to encrypt it:
C = P^e mod n = 113^101 mod 31571 = 5423

Alice uses her private key to decrypt it:
P = C^d mod n = 5423^13901 mod 31571 = 5423^(130*100+901) mod 31571 = 21223*10724 mod 31571 = 113

4) Suppose Alice sends plaintext P=113, how does she sign it and what are sent to Bob. How does Bob verify the signature?

Alice uses her private key to create a signature:
C = P^d mod n = 113^13901 mod 31571 = 113^(130*100+901) mod 31571 = 23843 * 26638 mod 31571 = 16027

Alice sends (P,S) = (113,16027) to Bob

Bob uses Alice's public key to verify the signature:
P' = C^e mod n = 16027^101 mod 31571 = 113

P' = P, the signature is verified.

5) Suppose Bob sends plaintext P=113, how does he sign it and what are sent to Alice. How does Alice verify the signature?

Bob uses his private key to create a signature:
C = P^d mod n = 113^10531 mod 19177 = 113^(100*100+531) mod 19177 = 12349 * 1653 mod 19177 = 8659

Bob sends (P,S) = (113, 8659) to Alice

Alice uses Bob's public key to verify the signature:
P' = C^e mod n = 8659^271 mod 19177 = 113

P' = P, the signature is verified.

4(1pt). In ElGammal, given the prime p = 1327, e1= 5, choose d=512 r=103.
a) Calculate e2 and encrypt the message "phone"; use 00 to 25 for encoding.
note: Each message to encrypt should be less than 1327, so you need to divide the message to letters and encrypt each letter independently.
pà15 hà7 oà14 nà13 eà4
P1 = 15
C1 = e1^r mod p = 5^103 mod 1327 = 1298
C2 = (P1 * e2^r) mod p = (15*1117^103) mod 1327 = 15* 437 mod 1327 = 1247
P2 = 7
C1 = 1298
C2 = (P2 * e2^r) mod p = (2*1117^103) mod 1327 = 7* 437 mod 1327 = 405
P3 = 14
C1 = 1298
C2 = (P3 * e2^r) mod p = (18*1117^103) mod 1327 = 14* 437 mod 1327 = 810
P4 = 13
C1 = 1298
C2 = (P4 * e2^r) mod p = (19*1117^103) mod 1327 = 13* 437 mod 1327 = 373
P5 = 4
C1 = 1298
C2 = (P4 * e2^r) mod p = (19*1117^103) mod 1327 = 4* 437 mod 1327 = 421
b) Suppose the receiver receives the following ciphertext pairs(c1,c2): (1298,421) (1298, 874) (1298, 1231) (1298, 341), describe how to decrypt them to find the original plaintext? (note: a and b are independent questions.)
P1 = [C2 * C1^(p-1-d)] mod p) =[421 * 1298^(1327-1-512)] mod 1327 = (421*1298^814) mod 1327 = (421*1078) mod 1327 = 4
P2 = (874*1078) mod 1327 = 2
P3 = (1231*1078) mod 1327 = 18
P4 = (341*1078) mod 1327 = 19
Plaintext: e c s t

5(1.5pt). Use the Rabin cryptosystem with p = 43 and q = 31
a) Encrypt P = 28 to find the ciphertext

n = pq = 43 * 31 = 1333
C = P^2 mod n = 28*28 mod 1333= 784 mod 1333

b) Use the Chinese Remainder Theorem to find four possible plaintexts

a1 = C^((p+1)/4) mod p = 784^(44/4) mod 43 = 15
a2 = - C^((p+1)/4) mod p = -15 mod 43 = 28 mod 43
b1 = C^((q+1)/4) mod q = 784^8 mod 31 = 28 mod 31
b2 = -28 mod 31 = 3

1)
x=15 mod 43
x=28 mod 31
a1=15, b1=28, m1=43, m2=31
M = 43*31 = 1333
M1 = 31, M2=43
$M1^{-1}$ mod m1 = 31^{-1} mod 43 = 31^{41} mod 43 = 25
$M2^{-1}$ mod m2 = 43^{-1} mod 31 = 43^{29} mod 31 = 13
x= (a1*M1* $M1^{-1}$ +b1*M2* $M2^{-1}$) mod M = (15*31*25 + 28*43*13) mod 1333 = (961 + 989) mod 1333 = 617

2)
x= 15 mod 43
x= 3 mod 31
a1=15, b2=3, m1=43, m2=31
M = 43*31 = 1333
M1 = 31, M2=43
$M1^{-1}$ mod m1 = 31^{-1} mod 43 = 31^{41} mod 43 = 25
$M2^{-1}$ mod m2 = 43^{-1} mod 31 = 43^{29} mod 31 = 13
x= (a1*M1* $M1^{-1}$ +b2*M2* $M2^{-1}$) mod M = (15*31*25 + 3*43*13) mod 1333 = (961 + 344) mod 1333 = 1305

3)
x= 28 mod 43
x= 28 mod 31
a2=15, b1=28, m1=43, m2=31
M = 43*31 = 1333
M1 = 31, M2=43
$M1^{-1}$ mod m1 = 31^{-1} mod 43 = 31^{41} mod 43 = 25
$M2^{-1}$ mod m2 = 43^{-1} mod 31 = 43^{29} mod 31 = 13
x= (a2*M1* $M1^{-1}$ +b1*M2* $M2^{-1}$) mod M = (28*31*25 + 28*43*13) mod 1333 = (372 + 989) mod 1333 = 28

4)
x= 28 mod 43
x= 3 mod 31
a2=28, b2=3, m1=43, m2=31
M = 43*31 = 1333
M1 = 31, M2=43
$M1^{-1}$ mod m1 = 31^{-1} mod 43 = 31^{41} mod 43 = 25
$M2^{-1}$ mod m2 = 43^{-1} mod 31 = 43^{29} mod 31 = 13
x= (a2*M1* $M1^{-1}$ +b2*M2* $M2^{-1}$) mod M = (28*31*25 + 3*43*13) mod 1333 = (372 + 344) mod 1333 = 716

6(1pt). ElGamal signature scheme. Let p=881, e1 = 3, d=61. The random value r is 7.

a) Find e2 and the signature of the message M=300.

e2 = e1^d mod p = 3^61 mod 881 = 589
S1 = e1^r mod p = 3^7 mod 881 = 425
φ(p-1) = φ(880) = φ(2^4 * 5 * 11) = (2^4-2^3) * 40 = 320
r^{-1} mod p-1 = 7^{-1} mod 880 = 7^{319} mod 880 = 503
S2 = (M – d*S1) r^{-1} mod p-1= (300 – 61*425)*503 mod 880 = 775 * 503 mod 880 = 865

c) Verify the signature (show all the intermediate results).

V1 = e1^M mod p = 3^300 mod 881 = 102
V2 = (e2^S1 * S1^S2) mod p = (589^425 * 425^865) mod 881 = 267 * 723 mod 881 = 102
V1 = V2, so the signature is verified.

7(1.5pt)DSS scheme. Let p = 787, q = 131, d = 57 and e0=5. Find values of e1 and e2. Choose r = 17.

1) Find the values of S1 and S2 if h(M) = 100.

e1 = e0^((p-1)/q) mod p = 5^6 mod 787 = 672 e2 = e1^d mod p = 672^57 mod 787 = 779

S1= e1^r mod p mod q = 672^17 mod 787 mod 131 = 62

S2 = (h(M) + dS1) r^{-1} mod q = (100 + 57 * 62) * 17^{129} mod 131 = 97 * 54 mod 131 = 129

2) Suppose the receiver receives (h(M), S1,S2) = (120, 57, 116). How to verify the signature(show all the intermediate results)?

Note: the signature has nothing to do with the signature created in a)

$S2^{-1}$ mod q = 116^{-1} mod 131 = 116^{129} mod 131 = 96

V = [e1^(h(M)*$S2^{-1}$) * e2^(S1*$S2^{-1}$) mod p mod q = [672^(120*96) * 779^(57*96)] mod 787 mod 131 = 672^516 * 779^756 mod 787 mod 131

= 213 * 689 mod 787 mod 131 = 375 mod 131 = 113

V != S1, so the signature is not verified.

8(0.5pt). In the Diifie-Hellman protocol, g = 11, p = 983.

a) Suppose Alice's private key is 45 and Bob's private key is 27, what are their public keys, respectively?

Alice’s public key: 11^45 mod 983 = 197

Bob’s public key: 11^27 mod 983 = 549

b) How does Alice calculate the shared key?

549^45 mod 983 = 358

c) How does Bob calculate the shared key?

197^27 mod 983 = 358