Eastern Mediterranean University
Computer Engineering Department
CMSE-353 Security of Software Systems
Final Exam

Six A4 sheets of handwritten paper may be used for your help. Photocopies, printouts, books, telephones, calculators, etc. are not allowed!

Duration: 180 Minutes **June 2, 2017**

Std Id_____ **Std Name**_____

Instructor Alexander Chefranov

Totally 12 questions, 100 points, 15 pages
Questions Q1-Q4 (33 points) cover before- and Q5-Q12 (67 points) after-MT material

Question (max point)	Q1 (5)	Q2 (6)	Q3 (11)	Q4 (11)	Q5 (10)	Q6 (8)	Q7 (6)	Q8 (12)	Q9 (3)	Q10 (12)	Q11 (6)	Q12 (10)	Total (100)
Point													

Q1. (5 points) What <u>five</u> types of malicious software do you know? What is a Trojan horse? How does it enter a victim computer?

- Backdoors
- logic bombs
- Computer viruses
- Computer worms
- Trojan horse

Trojan horse is a malicious software looking innocent and attractive for a victim. A victim attracted by the program (e.g., game), installs it herself on her computer.

Q2 (6 points). What is One-Time Pad (OTP)? How does it work? Keys of what size are used in OTP? Is OTP a block or stream cipher? Why OTP is considered unconditionally secure?

OTP encrypt the plaintext byte stream by XOR-ing with the key byte stream. A key byte-stream is generated entirely new for each new plaintext. OTP is a stream cipher. Key size is equal to the plaintext size. OTP is considered unconditionally secure because for any cipher-text and any supposed plaintext, it is possible finding a key such that the plaintext is converted to the given ciphertext.

Q3 (11 points). Use Hill cipher to encrypt and decrypt back the message "ABC", if the key matrix

K=

17	17	5
21	18	21
2	2	19

, its inverse is

K^{-1}=

4	9	15
15	17	6
24	0	17

and the alphabet is coded as follows:

a	b	c	d	e	f	g	H	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Check that the matrices are actually reciprocals; show necessary computations, give explanations. What modulo value shall be used in the calculations? What is the block size for that Hill cipher variant?

Block size is 3. Modulo 26 shall be used. $K \cdot K^{-1}$ shall be equal to the unity matrix. Let's check it

$$\begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 15 \end{vmatrix} \cdot \begin{vmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{vmatrix} \bmod 26 =$$

$$= \begin{vmatrix} 68+255+120 & 153+289+0 & 255+102+85 \\ 84+210+504 & 189+306+0 & 315+408+357 \\ 8+30+456 & 18+34+0 & 30+12+325 \end{vmatrix} =$$

$$= \begin{vmatrix} 443 & 442 & 442 \\ 798 & 495 & 1080 \\ 494 & 52 & 367 \end{vmatrix} =$$

$$= \begin{vmatrix} 16+21+16 & 23+3+0 & 21+24+7 \\ 24+10+18 & 4+20+0 & 3+4+19 \\ 8+4+14 & 52 & 4+12+11 \end{vmatrix} =$$

$$= \begin{vmatrix} 53 & 26 & 52 \\ 52 & 27 & 26 \\ 26 & 52 & 27 \end{vmatrix} \bmod 26 = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} = \text{unity matrix}$$

Check:

$$\begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix} \begin{vmatrix} 0 \\ 1 \\ 2 \end{vmatrix} \bmod 26 = \begin{vmatrix} 0+17+10 \\ 0+18+42 \\ 0+2+38 \end{vmatrix} = \begin{vmatrix} 27 \\ 60 \\ 40 \end{vmatrix} = \begin{vmatrix} 1 \\ 8 \\ 14 \end{vmatrix}$$

$= (B\ I\ O)$

Decr:

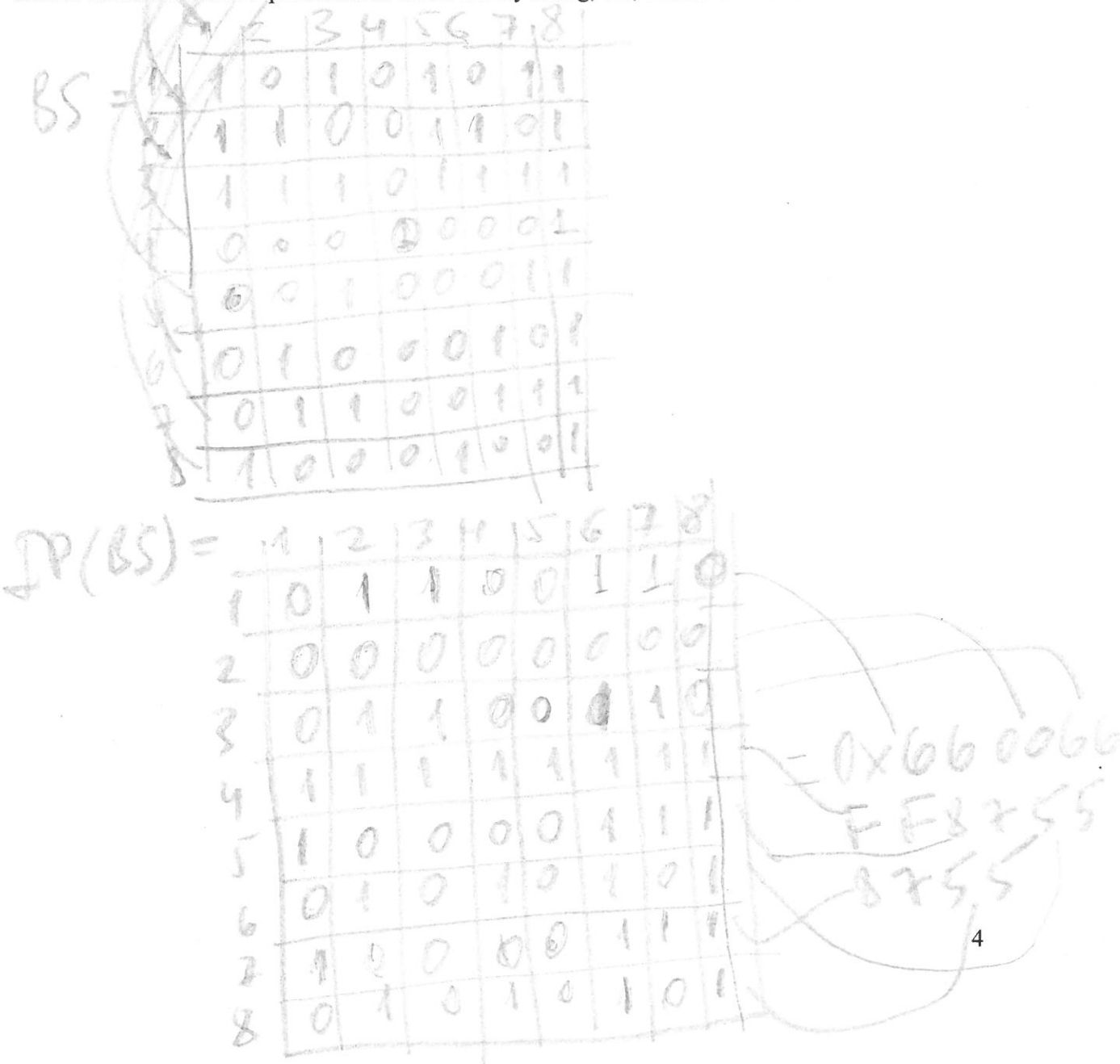
$$\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} 1 \\ 8 \\ 14 \end{pmatrix} \bmod 26 = \begin{pmatrix} 4+72+210 \\ 15+136+84 \\ 24+0+238 \end{pmatrix} = \begin{pmatrix} 286 \\ 5+6 \\ 262 \end{pmatrix}$$

$$= \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} A \\ B \\ C \end{pmatrix} = \text{plaintext}$$

Q4 (11 points). Apply DES Initial Permutation, IP

IP
58 50 42 34 26 18 10 2
60 52 44 36 28 20 12 4
62 54 46 38 30 22 14 6
64 56 48 40 32 24 16 8
57 49 41 33 25 17 9 1
59 51 43 35 27 19 11 3
61 53 45 37 29 21 13 5
63 55 47 39 31 23 15 7

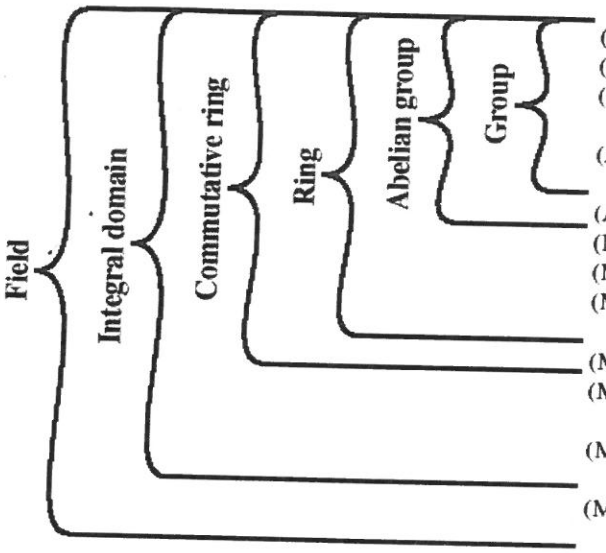
to the following binary string, BS, represented in hexadecimal:
BS=0x AB CD EF 01 23 45 67 89
Show your work, explain it, represent the result in hexadecimal
HINT: Use 8x8 matrix representation of the binary string, BS, similar to that of IP.



Q5. (10 points) What is a ring? What is a field? Is ring a field? Why? Is field a ring? Why? Give example of a

- ring
- field.

Prove that the examples are actually a ring and a field.
HINT:



(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Figure 4.1 Group, Ring, and Field

A ring is a set R with operations + and × defined on it. Operations + and × are group operations. Properties A1-A5 and M1-M3 hold. For a field, additionally properties M4-M7 hold. Generally ring is not a field since M4-M7 may not be true for a ring. Field is a ring. Since A1-A5 and M1-M3 hold for a field. $\mathbb{Z}_8$ with + and × is a ring. $\mathbb{Z}_7$ with + and × is a field (since every element in $\mathbb{Z}_7$ has a multiplicative inverse). For $\mathbb{Z}_8$, e.g. 2 has not a multiplicative inverse

Q6. (8 points) Calculate $12^{34} \bmod 56$, show your intermediate calculations

$12^{34} \bmod 56 = 12^{32} \cdot 12^2 \bmod 56$

$12^2 \bmod 56 = 144 \bmod 56 = 32$

$12^4 \bmod 56 = 32^2 \bmod 56 = 64 \cdot 16 \bmod 56 =$

$8 \cdot 16 \bmod 56 = 128 \bmod 56 = 16$

$12^8 \bmod 56 = 16^2 \bmod 56 = 64 \cdot 4 \bmod 56 =$

$= 32$

$12^{16} \bmod 56 = 32^2 \bmod 56 = 16$

$12^{32} \bmod 56 = 16^2 \bmod 56 = 32$

$12^{34} \bmod 56 = 32 \cdot 32 = 64 \cdot 16 \bmod 56$

$= 8 \cdot 16 \bmod 56 = 128 \bmod 56 = 16$

Hence, $12^{34} \bmod 56 = 16$

Q7. (6 points) What is a Greatest Common Divisor (GCD)? Find GCD(1234, 567) using Euclid's algorithm. Show your calculations.
HINT:

EUCLID(a,b)

1. A:=a; B:=b
2. if B=0 return A=gcd(a,b)
3. R=A mod B
4. A:=B
5. B:=R
6. goto 2

$A = 1234, B = 567$

$R = A \bmod B =$ 1234 | 567
1134 2
100

$A = 567, B = 100$

$R = A \bmod B = 567 \bmod 100 = 67$

$A = 100, B = 67$

$R = A \bmod B = 100 \bmod 67 = 33$

$A = 67, B = 33$

$R = A \bmod B = 67 \bmod 33 = 1$

$A = 33, B = 1$

$R = 33 \bmod 1 = 0$

$A = 1, B = 0 \rightarrow gcd(1234, 567) = 1$

Q8. (12 points) Use Extended Euclid's Algorithm to calculate $(x^7+x+1)^{-1}$ in GF(2^8) with m(x)= $x^8+x^4+x^3+x+1$. Check correctness of your calculations by multiplication. Show your intermediate results.

HINT:

EXTENDED EUCLID[m(x),b(x)]

1. [A1(x), A2(x), A3(x)]:=[1,0,m(x)]; [B1(x), B2(x), B3(x)]:=[0,1,b(x)];
2. if B3(x)=0 return A3(x)= gcd[m(x),b(x)]; no inverse
3. if B3(x)=1 return B3(x)= gcd[m(x),b(x)]; B2(x)=b(x)$^{-1}$ mod m(x)
4. Q(x):= quotient of A3(x)/B3(x)
5. [T1(x), T2(x), T3(x)]:= [A1(x)-QB1(x), A2(x) –QB2(x), A3(x) –QB3(x)]
6. [A1(x), A2(x), A3(x)]:= [B1(x), B2(x), B3(x)]
7. [B1(x), B2(x), B3(x)]:= [T1(x), T2(x), T3(x)]
8. goto 2

$A=(1,0,x^8+x^4+x^3+x+1)$ $B=(0,1,x^7+x+1)$

$Q=x$

x^8+x^2+x

$x^4+x^3+x^2+1$

$T=A-QB=(1,x,x^4+x^3+x^2+1)$

$A=(0,1,x^7+x+1)$ $B=(1,x,x^4+x^3+x^2+1)$

$Q=x^3+x^2+1$

$x^7+x^6+x^5+x^3$

$x^6+x^5+x^4+x^2$

$x^4+x^3+x^2+x+1$

$x^4+x^3+x^2+1$

1

$T=A-QB=(x^3+x^2+1,\ 1+x(x^3+x^2+1),\ x)=$

$=(x^4+x^2+1,\ 1+x^4+x^3+x,\ x)=$

$=(x^4+x^3+x^2+1,\ x^4+x^3+x+1,\ x)$

$A = (1, x, x^4+x^3+x^2+1)$, $B = (x^3+x^2+1,$
$x^4+x^3+x+1, x)$

$Q = x^4+x^3+x^2+1 \;\big|\; x$
$\underline{x^4}$
x^3+x^2+1
$\underline{x^3}$
x^2+1
$\underline{x^2}$
1 (1)

$T = A - QB = (1, +(x^3+x^2+x)(x^3+x^2+1),$
$x+(x^3+x^2+x)(x^4+x^3+x+1), 1)$

Since $B = T$ & $B3 = 1 \to (x^7+x+1)^{-1} =$

$x+(x^3+x^2+x)(x^4+x^3+x+1) = x+x^7+x^6+x^5+$
$+x^4+x^5+x^4+x^4+x^3+x^2+x^3+x^2+x = x^7$

Check that the result is true:

$(x^7+x+1)\cdot x^7 = x^{14}+x^8+x^7 \;\big|\; x^8+x^4+x^3+x+1$
$\underline{x^{14}+x^{10}+x^9+x^7+x^6}$ x^6+x^2+x+1
$x^{10}+x^9+x^8+x^6$
$\underline{x^{10}+x^6+x^5+x^3+x^2}$
$x^9+x^8+x^5+x^3+x^2$
$\underline{x^9+x^5+x^4+x^2+x}$
$x^8+x^4+x^3+x$
$\underline{x^8+x^4+x^3+x+1}$
1 (1)

Since the remainder obtained $= 1$,
actually $(x^7+x+1) \bmod (x^8+x^4+x^3+x+1) =$
$= x^7$

Q9. (3 points) What is the result of AES S-box substitution, S(w), for w=0xAB (in hexadecimal). Give necessary explanations
HINT:

Table 5.4 AES S-Boxes

(a) S-box

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

(b) Inverse S-box

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

S(0xAB) = 0x62

The first hexadecimal digit is a row number and the second hexadecimal digit defines a column, on the cross of which the target value is found

Q10. (12 points) Use RSA to encrypt and decrypt back m=14 if N=77. Define yourself all necessary ingredients of RSA, give necessary explanations

HINT:

RSA (Rivest-Shamir-Adelman, 1978) algorithm is an asymmetric encryption algorithm. To design an encryption/decryption key pair, two large prime numbers, p and q, $p \neq q$, are selected, and an integer, d, is chosen that is relatively prime to (p-1)(q-1) (d and (p-1)(q-1) have no common factors other than 1). Finally, an integer e is computed such that

$$e \cdot d \equiv 1(\mathrm{mod}(p-1)\cdot(q-1))$$

One key is (e,N), and the other is (d,N), where N=p*q, and is referred to as the modulus.

For example, we might select p=7, and q=13. Then N=91, and (p-1)(q-1)=72. We can choose d=5 (which is relatively prime to 72) and e=29, because e*d=145 and

$$145 \equiv 1(\mathrm{mod}\ 72)$$

Then, one key is K_1=(29,91) and the other is K_2=(5,91). The message to be encrypted is broken into blocks such that each block, M, can be treated as an integer between 0 and (N-1). To encrypt M into the ciphertext block, B, we perform

$$B = M^{K_1} (\mathrm{mod}\, N)$$

To decrypt B, we perform

$$M = B^{K_2} (\mathrm{mod}\, N)$$

$N = 77 = p \cdot q \Rightarrow p = 7, q = 11$

$\varphi(N) = (p-1)(q-1) = 6 \cdot 10 = 60$

$e \cdot d = 1 \bmod \varphi(N) = 1 \bmod 60$

$e = 7$, $\gcd(7, 60) = 1 \rightarrow e^{-1} = d$ exists

$d = e^{-1} \bmod 60 =$

$A = (1, 0, 60)$, $B = (0, 1, 7)$

$Q = 60 \,/\, 7$

$56 \quad 8$

4

$T = A - QB = (1, -8, 4)$

$A = (0, 1, 7)$, $B = (1, -8, 4)$

$Q = 7 \,/\, 4$

$4 \quad 1$

3

$T = (-1, 9, 3)$

$A = (1, -8, 4)$, $B = (-1, 9, 3)$

$Q = \begin{matrix} 4 & \lfloor \frac{3}{1} \\ \frac{3}{1} & \end{matrix}$

$T = A - QB = (2, -17, 1)$

Since new $B = T$, $BS = 1$, hence, $7^{-1} = -17 \bmod 60 = 43$. Check it:

$7 \cdot 43 = 301 = 5 \cdot 60 + 1 \bmod 60 = 1$

Hence, $d = 43$

$C = m^e \bmod 77 = 14^7 \bmod 77$

$14^2 \bmod 77 = 196 \bmod 77 = 42$

$14^4 = 42^2 \bmod 77 = 84 \cdot 21 \bmod 77 = 7 \cdot 21 =$

$= 147 \bmod 77 = 70$

$C = 14^7 = 14 \cdot 14^2 \cdot 14^4 = 14 \cdot 42 \cdot 70 \bmod 77 =$

$= 7 \cdot 84 \cdot 70 \bmod 77 = 49 \cdot 70 \bmod 77 = 98 \cdot 35 \bmod 77$

$= 21 \cdot 35 \bmod 77 = 105 \cdot 7 \bmod 77 = 28 \cdot 7 = 98 \cdot 2 = 42$

Decrypt $42^{43} = 42^{32} \cdot 42^8 \cdot 42^2 \cdot 42$

$42^2 \bmod 77 = 84 \cdot 21 \bmod 77 = 7 \cdot 21 \bmod 77 = 70$

$42^4 \bmod 77 = 70^2 \bmod 77 = 140 \cdot 35 \bmod 77 = 63 \cdot 35$

$\bmod 77 = 9 \cdot 245 \bmod 77 = 9 \cdot 14 = 126 \bmod 77 = 49$

$42^8 \bmod 77 = 49 \cdot 49 \bmod 77 = 343 \cdot 7 \bmod 77 =$

$= 35 \cdot 7 \bmod 77 = 245 \bmod 77 = 14$

$42^{16} \bmod 77 = 14^2 \bmod 77 = 196 \bmod 77 = 42$

$42^{32} = 70$

$C^d = 42^{32} \cdot 42^8 \cdot 42^2 \cdot 42 = 70 \cdot 14 \cdot 70 \cdot 42 \bmod 77 = 49 \cdot 42 \cdot 3$

$\bmod 77 = 98 \cdot 21 \cdot 3 \bmod 77 = 21 \cdot 21 \cdot 3 \bmod 77 = 147 \cdot 9 \bmod 77$

$= 70 \cdot 9 \bmod 77 = 630 \bmod 77 = 14 = m$

Q11. (6 points) What a digital signature is? How a hash function is used in the digital signature? How a digital signature is verified? What a certificate is? What a Certificate Authority is? What three checks are made to verify a certificate?

Let E is an asymmetric cipher with the private key, R, and public key, P. h is a hash function, m is a message to be signed. Then Digital signature, DS(m), of the message, m, is

$$DS(m) = E_R(h(m))$$

Digital signature is verified as follows. Let receiver gets a message m' with signature, ds'. Then, the receiver checks,

$$D_P(ds') == h(m'),$$

where D - is the decryption method for the encryption method, E.

A certificate is a document stating subject name, affiliation, and his public key, that is digitally signed by a Certificate Authority. Certificate authority is a person / organization authorized to issue certificates. In addition to the signature, certificates is verified versus expiration date and revoka-

Q12. (10 points). Given N=5, h(x)=(2*x+5)^{2}mod17, what will be the initial record for the user A in the Lamport's One-Time Password scheme? What password shall be provided by A when the first time being authenticated by the server, S, and what will be the new record of A in the S's database after the first successful A authentication. Give necessary explanations for your answers.
HINT:

Initialization Procedure

The client selects a password, p_0, a number, N, calculates

$$p_N = h^N(p_0),$$

where

$$h^{i+1}(x) = h(h^i(x)), h^0(x) = x.$$

The client securely delivers to the server (N, p_N), and the servers saves it into ($Counter, password, Client\_ID$) tuple.

Authentication Procedure

When the client, C, requests authentication by the server, S, the following proceeds:

1. C -> S: C_ID //client sends his ID
2. S -> C: Counter(C_ID) //server responds by respective Counter value
3. C -> S: C_ID, $pwd_{Counter} = h^{Counter-1}(p_0)$
4. S: If $h(pwd_{Counter}) == password(C\_ID)$ then {

S authenticates C, and sets $(Counter, password, \_ID) = (Counter-1, pwd_{Counter}, C\_ID)$

}
Else C is not authenticated

Let $p_0 = 2$. Then

$h(p_0) = (2\cdot 2+5)^2 \bmod 17 = 9^2 \bmod 17 = 81 \bmod 17 = 13$

$h^2(p_0) = (2\cdot 13+5)^2 \bmod 17 = 31^2 \bmod 17 = 14^2 \bmod 17 = 28\cdot 7 \bmod 17 = 11\cdot 7 \bmod 17 = 9$

$h^3(p_0) = (2\cdot 9+5)^2 \bmod 17 = 23^2 \bmod 17 = 36 \bmod 17 = 2$

$h^4(p_0) = h(2) = 13$

$h^5(p_0) = h(13) = 9$

Initial record is $(5, 9, A)$

When authenticated for the third time, A provides the following password

$pwd = h^4(pw) = 13$ as an answer on the challenge from the server that is equal to 5.

After authentication, the new A's record will be

$(4, 13, A)$

Since the counter in the first field of A's record is decremented, and the password, pwd, sent by A, becomes a new password in the A's record.