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 **January 5, 2018**

Std Id_____ **Std Name**_____

Instructor Alexander Chefranov

Totally 15 questions, 105 points (5 bonus points, maximum 100 points will be used for grading), 17 pages
Questions Q1-Q4 (33 points) cover before- and Q5-Q15 (72 points) after-MT material

Question (max point)	Q1 (5)	Q2 (6)	Q3 (11)	Q4 (11)	Q5 (6)	Q6 (7)	Q7 (6)	Q8 (8)	Q9 (8)	Q10 (8)	Q11 (6)	Q12 (6)	Q13 (4)	Q14 (8)	Q15 (5)	Total (105)
Point																

Q1. (5 points) What is a macrovirus? How infection by the Melissa macrovirus happens? What event is used for the Melissa macrovirus activation?

Macrovirus is a virus written in Visual Basic for Applications
Infection by Melissa happens when an infected file is opened
The event is Document.Open

Q2 (6 points). What is the Ceasar cipher? How does it work? How many key it has? Specify its substitution table for some key. For the key you select, encrypt and decrypt back the following plaintext: "PLAIN". Give necessary explanations.

Ceasar copper is a substitution cipher
It works by substituting a plaintext letter
by a cipertext letter. It has 25 keys.

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

$K = 3$ $\quad c = (p+3) \bmod 26$

$p = (C-B) \bmod 26$

PLAIN $\Leftrightarrow$ 15 11 0 8 13 $\Leftrightarrow$ 18 14 3 11 16

$\Leftrightarrow$ S O D L Q $\leftarrow$ ciphertext

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

K=

1	2
3	4

block size = 2

$n = 27$

and the 27-element alphabet including ' ' 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	26

Check existence of the inverse key matrix and find it. Show your calculations, give necessary explanations. What modulo value shall be used in the calculations? What is the block size for that Hill cipher variant?

$\det k = 1 \cdot 4 - 2 \cdot 3 = 4 - 6 = -2 \bmod 27 = 25 \neq 0$

$\gcd(\det k, n) = \gcd(25, 27) = 1 \rightarrow k$ is invertible

$(\det k)^{-1} = 25^{-1} \bmod 27 = (-2)^{-1} \bmod 27 = -14 \bmod 27 =$

$= 13$. Actually $13 \cdot 25 = 325 \bmod 27 = (12 \cdot 27 + 1) \bmod 27 = 1$

$$K^{-1}_{(ij)} = \frac{1}{\det K} A_{ji} \cdot (-1)^{i+j} \bmod n$$

$$K^{-1}_{11} = 13 \cdot (-1)^2 \cdot 4 \bmod 27 = 25 = -2$$

$$K^{-1}_{12} = 13 \cdot (-1)^3 \cdot 2 \bmod 27 = -26 \bmod 27 = 1$$

$$K^{-1}_{21} = 13 \cdot (-1)^3 \cdot 3 \bmod 27 = -12 \bmod 27 = 15$$

$$K^{-1}_{22} = 13 \cdot (-1)^2 \cdot 1 \bmod 27 = 13$$

$$K^{-1} = \begin{vmatrix} -2 & 1 \\ 15 & 13 \end{vmatrix}$$

$$K^{-1} \cdot K = \begin{vmatrix} -2 & 1 \\ 15 & 13 \end{vmatrix} \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = \begin{vmatrix} -2+3 & -4+4 \\ 15+39 & 30+52 \end{vmatrix} \bmod 27$$

$$= \begin{vmatrix} 1 & 0 \\ 54 & 82 \end{vmatrix} \bmod 27 = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}$$

"PLAN" $= (15\ 11)(0\ 26)$

$$C_1 = K \cdot \begin{vmatrix} 15 \\ 11 \end{vmatrix} = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} \begin{vmatrix} 15 \\ 11 \end{vmatrix} \bmod 27 = \begin{pmatrix} 15+22 \\ 45+44 \end{pmatrix} \bmod 27$$

$$= \begin{pmatrix} 37 \\ 89 \end{pmatrix} \bmod 27 = \begin{pmatrix} 10 \\ 8 \end{pmatrix} = (K\ I)$$

$$C_2 = K \cdot \begin{vmatrix} 0 \\ 26 \end{vmatrix} = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} \begin{vmatrix} 0 \\ 26 \end{vmatrix} = \begin{pmatrix} 0+52 \\ 0+104 \end{pmatrix} \bmod 27 =$$

$$= \begin{pmatrix} 25 \\ 23 \end{pmatrix} = (Z\ X) \rightarrow C = (K\ I\ Z\ X)$$

$$P_1 = K^{-1} \cdot \begin{pmatrix} 10 \\ 8 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 15 & 13 \end{pmatrix} \begin{pmatrix} 10 \\ 8 \end{pmatrix} = \begin{pmatrix} -20+8 \\ 150+104 \end{pmatrix} \bmod 27 =$$

$$= \begin{pmatrix} -12 \\ 254 \end{pmatrix} \bmod 27 = \begin{pmatrix} 15 \\ -16 \end{pmatrix} \bmod 27 = \begin{pmatrix} 15 \\ 11 \end{pmatrix} = (P\ L)$$

$$P_2 = K^{-1} \begin{pmatrix} 25 \\ 23 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 15 & 13 \end{pmatrix} \begin{pmatrix} -2 \\ -4 \end{pmatrix} \bmod 27 = \begin{pmatrix} 4-4 \\ -30-52 \end{pmatrix} = \begin{pmatrix} 0 \\ -82 \end{pmatrix}$$

$$\bmod 27 = \begin{pmatrix} 0 \\ -1 \end{pmatrix} \bmod 27 = \begin{pmatrix} 0 \\ 26 \end{pmatrix} = (A\ N) \rightarrow \text{"PLAN"}$$

Q4 (11 points). Apply DES Permutation, P

	Permutation function(P)
1	16 7 20 21 29 12 28 17
2	1 15 23 26 5 18 31 10
3	2 8 24 14 32 27 3 9
4	19 13 30 6 22 11 4 25

to the following binary string, BS, represented in hexadecimal:
BS=0x AC DB FA 49
Show your work, explain it, represent the result in hexadecimal. Give necessary explanations.
HINT: Use 4x8 matrix representation of the binary string, BS, similar to that of P.

$$BS = \begin{vmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{vmatrix}$$

$$P(BS) = \begin{vmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{vmatrix} =$$

$$= BDFD0B\Delta0$$

Q5. (6 points) Find inverse of the following permutation p=(1,3,5,2,4). Give necessary definitions and explanations

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix} \qquad p \cdot p^{-1} = I$$

$$p^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}$$

$p \cdot p^{-1} = (1\,3\,5\,2\,4)(1\,4\,2\,5\,3) = (1\,2\,3\,4\,5)$

p^{-1} is correct since $p \cdot p^{-1}$ returns the identity permutation, I

Q6. (7 points) Calculate $31^{31} \bmod 54$, show your intermediate calculations. Give necessary explanations.

$31^2 \bmod 54 = 900 + 60 + 1 = 961 \equiv 43$

$31^4 = 43^2 \bmod 54 = 1600 + 240 + 9 = 1849 \equiv 13$

$31^8 = 13^2 = 169 \bmod 54 = 7$

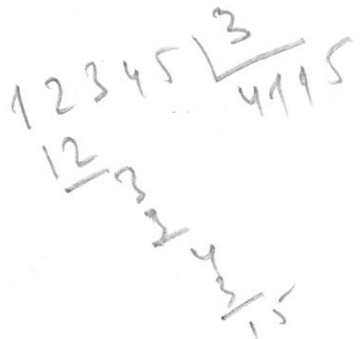
$31^{16} = 07^2 = 49$

$31^{31} = 31^{16} \cdot 31^8 \cdot 31^4 \cdot 31^2 \cdot 31 = 49 \cdot 7 \cdot 13 \cdot 43 \cdot 31 =$

$= 49 \cdot 91 \cdot 43 \cdot 31 = 49 \cdot 37 \cdot 43 \cdot 31 = 1 \cdot 37 \cdot 31 = (30+7)(30+1)$

$= 900 + 210 + 30 + 7 = 1147 \bmod 54 = 13$

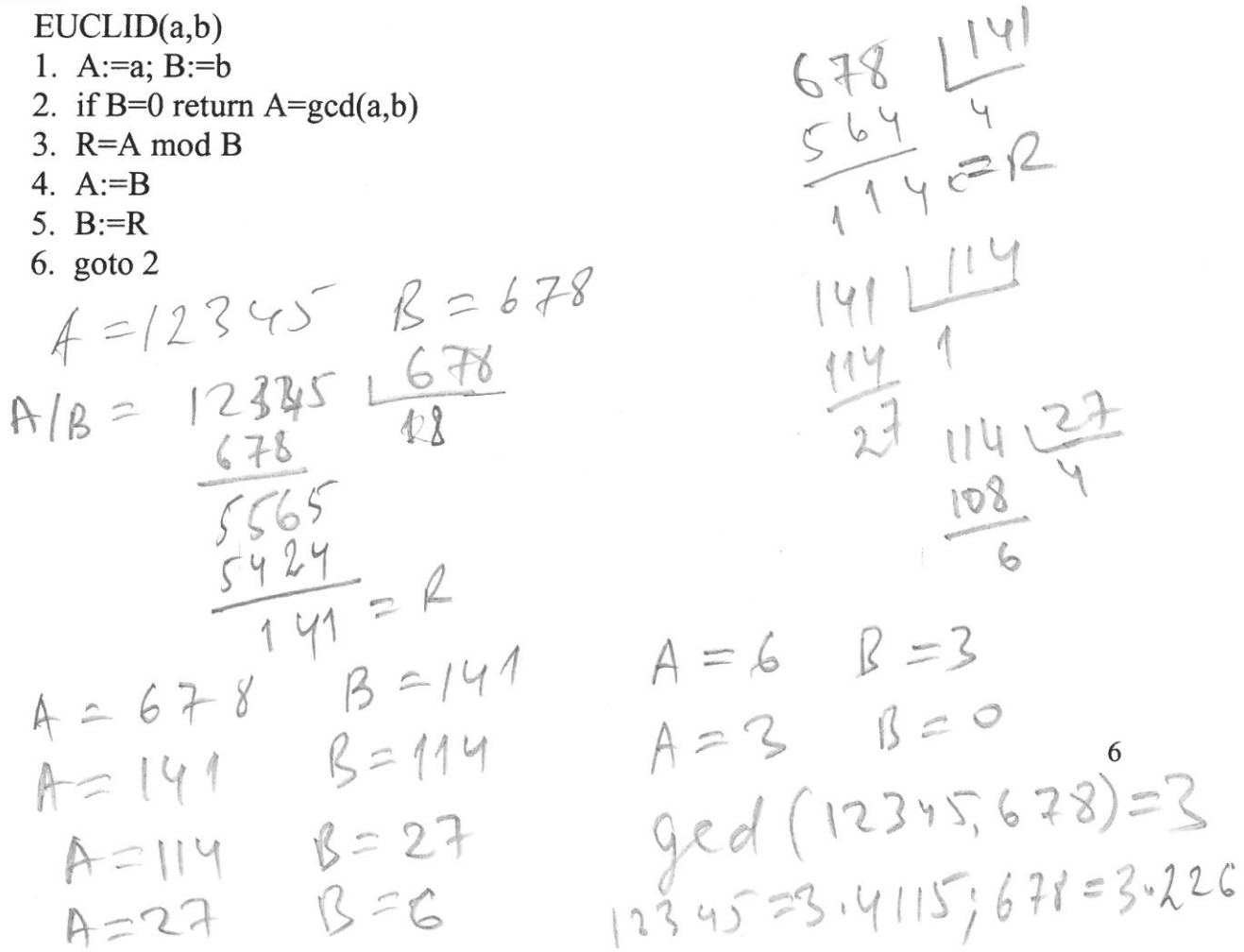
We use: $a \cdot b \bmod u = \big((a \bmod u)(b \bmod u)\big) \bmod u$



Q7. (6 points) What is a Greatest Common Divisor (GCD)? Find GCD(12345, 678) using Euclid's algorithm. Show your calculations. Give necessary explanations.
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



$T = A - QB = (1 - 0 \cdot Q,\ 0 - Q \cdot 1,\ x^3 + x^2 + x + 1) =$

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

$A = (0, 1,\ x^6 + x^2 + 1)$, $B = (1, x^2,\ x^3 + x^2 + x + 1)$

$Q = x^6 + x^2 + 1 \ \big|\ x^3 + x^2 + x + 1$

$x^6 + x^5 + x^4 + x^3 \quad\quad x^3 + x^2$

$x^5 + x^4 + x^3 + x^2 + 1$

$x^5 + x^4 + x^3 + x^2$

1

$T = A - QB = (0 - Q,\ 1 - Q \cdot x^2,\ 1) =$

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

$A = (1, x^2, x^3 + x^2 + x + 1)$, $B = (x^3 + x^2,\ x^5 + x^4 + 1,\ 1)$

$B2 = 1 \Rightarrow B2 = (x^6 + x^2 + 1)^{-1} = x^5 + x^4 + 1 = B^{-1} \rightarrow$ next page →

Q8. (8 points) Use Extended Euclid's Algorithm to calculate $(x^6 + x^2 + 1)^{-1}$ 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. Give necessary explanations.

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

$A = (1, 0, x^8 + x^4 + x^3 + x + 1)$, $B = (0, 1, x^6 + x^2 + 1) = B$

$Q = x^8 + x^4 + x^3 + x + 1 \ \big|\ x^6 + x^2 + 1$

$x^8 + x^4 + x^2 \quad\quad x^2$

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

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

Check that $b^{-1} \cdot b \bmod m = 1$

$(x^5+x^4+1)(x^6+x^2+1) = x^{11}+x^7+x^5+$

$+x^{10}+x^6+x^4+x^6+x^2+1 = x^{11}+x^{10}+x^7+x^5+x^4+$

$+x^2+1$

$x^{11}+x^{10}+x^7+x^5+x^4+x^2+1 \;\big|\; x^8+x^4+x^3+x+1$

$x^{11}+x^7+x^6+x^4+x^3$ — x^3+x^2

$x^{10}+x^6+x^5+x^3+x^2+1$

$x^{10}+x^6+x^5+x^3+x^2$

1

Hence, $b^{-1} \bmod m = x^5+x^4+1$

Q9. (8 points) For the Mix Column Transformation explained below on an example, provide calculations showing that actually, S10'=37. Irreducible polynomial used in AES is m(x)= $x^8 + x^4 + x^3 + x + 1$. Give necessary explanations.

"The forward mix column transformation, called MixColumns, operates on each column individually. Each byte is mapped into a new value that is a function of all four bytes in the column. The transformation can be defined as the following matrix multiplication on State (Fig. 5.5b):

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

*

S00	S01	S02	S03
S10	S11	S12	S13
S20	S21	S22	S23
S30	S31	S32	S33

=

S00'	S01'	S02'	S03'
S10'	S11'	S12'	S13'
S20'	S21'	S22'	S23'
S30'	S31'	S32'	S33'

(5.3)

Each element in the product matrix is the sum of products of elements of one row and one column. In this case, multiplications and additions are performed in GF(2^8).

The following is the example of MixColumns;

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

=>

47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC

"

$\{01\}\cdot\{87\} + \{02\}\cdot\{6E\} + \{03\}\{46\} + \{01\}\cdot\{A6\}$

$\{01\}\{87\} = 87$

$\{02\}\{6E\} = \{00000010\}\{01101110\} =$

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

$= (11011100) = \{DC\}$

$\{03\}\{46\} = \{00000011\}\{01000110\} =$

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

$= x^7 + x^6 + x^3 + x = (11001010) = \{CA\}$

$\{01\}\{A6\} = A6$

$87 + DC + CA + A6 =$

$= 10000111$
11011100
11001010
10100110

$00110111 = 37$

Q10. (8 points) Use RSA to encrypt and decrypt back m=16 if N=55. 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

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

$N = 55 = pq = 11 \cdot 5$ $p = 11$ $q = 5$

$\varphi(N) = (p-1)(q-1) = 10 \cdot 4 = 40$

$e = 3$; $\gcd(e, \varphi(N)) = \gcd(3, 40) = 1$

$d = e^{-1} \bmod \varphi(N) = 3^{-1} \bmod 40 = 27$

$e \cdot d = 3 \cdot 27 \bmod 40 = 81 \bmod 40 = 1$

$A = (1, 0, 40)$ $B = (0, 1, 3)$

$q = A3/B3 = \lfloor 40/3 \rfloor = 13$

$T = A - qB = (1, -13, 1) \rightarrow 3^{-1} = -13 \bmod 40 = 27$

$C = m^e \bmod N = 16^3 \bmod 55 =$

$16^2 \bmod 55 = 256 \bmod 55 = (4 \cdot 55 + 36) \bmod 55$

$= 36$

$16^3 = 36 \cdot 16 \bmod 55 = 72 \cdot 8 \bmod 55 = 17 \cdot 8 \bmod 55$

$= 68 \cdot 2 \bmod 55 = 13 \cdot 2 \bmod 55 = 26 = C$

$m' = c^{27} \bmod 55 = 26^{27} \bmod 55$

$26^2 \bmod 55 = 169 \cdot 4 \bmod 55 = (3 \cdot 55 + 4) \cdot 4 \bmod 55$

$= 16$

$26^4 = 16^2 \bmod 55 = 36$

$26^8 = 36^2 \bmod 55 = 81 \cdot 16 \bmod 55 = 26 \cdot 16 \bmod 55 =$

$= 104 \cdot 4 \bmod 55 = (2 \cdot 55 - 6) \cdot 4 \bmod 55 = -24 \bmod 55$

$= 31$

$26^{16} = 31^2 \bmod 55 = 961 \bmod 55 = 26$

$961 : 55 = 17$

55

411

385

26

$26^{27} = 26^{16} \cdot 26^8 \cdot 26^2 \cdot 26 = 26 \cdot 31 \cdot 16 \cdot 26 =$

$= 26^2 \cdot 31 \cdot 16 = 16 \cdot 31 \cdot 16 = 16^2 \cdot 31 = 36 \cdot 31 =$

$= 18 \cdot 62 \bmod 55 = 18 \cdot 7 \bmod 55 = 2 \cdot 63 \bmod 55 =$

$= 2 \cdot 8 = 16 = m$

Q11. (6 points) How a digital signature is constructed? How a digital signature is verified? Give an example of a message and its RSA signature using hash function h(x)=x mod 11. Give necessary definitions and explanations.

$DS(M) = M\ E_R(h(M))$

Verification $h(M') = = D_p(E_R(h(M)))$

$M = 16 \quad h(M) = 5$

$R = 3 \quad P = 27 \quad N = 55$ (take from Q10)

$E_R(h(M)) = 5^3 \bmod 55 = 125 \bmod 55 =$

$= 15$

$DS(M) = 16, 15 = M'$, signature

Verification

$h(M') = 5$;

$D_p(\text{signature}) = 15^{27} \bmod 55 =$

$15^2 = 225 \bmod 55 = 5$

$15^4 = 5^2 \bmod 55 = 25$

$15^8 = 25^2 \bmod 55 = 125 \cdot 5 \bmod 55 = 15 \cdot 5 = 75 =$

$= 20$

$15^{16} = 20^2 \bmod 55 = 25 \cdot 16 = 100 \cdot 4 \bmod 55 =$

$= 45 \cdot 4 \bmod 55 = 180 \bmod 55 = 15$

$15^{27} = 15^{16} \cdot 15^8 \cdot 15^2 \cdot 15 = 15 \cdot 20 \cdot 5 \cdot 15 \bmod 55 =$

$= 15 \cdot 20 \cdot 20 \bmod 55 = 15 \cdot 15^2 \bmod 55 = 15^3 \bmod 55$

$= 5$

$h(M') = = D_p(\text{signature})$ is true

$5 = 5$

Q12. (6 points). Given N=6, h(x)=(3*x+4)^{2}mod19, 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:

9 not 4

xxxx

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.

9 not 4

xxx

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

$p_0 = 2$

$p_1 = h(p_0) = (3\cdot 2+4)^2 \bmod 19 = 100 \bmod 19 = 5$

$p_2 = h(p_1) = (3\cdot 5+4)^2 \bmod 19 = 0$

$p_3 = h(p_2) = (3\cdot 0+4)^2 \bmod 19 = 16$

$p_4 = h(p_3) = (3\cdot 16+4)^2 = 52^2 \bmod 19 = 14^2 \bmod 19 = 6$

$p_5 = h(p_4) = (3\cdot 6+4)^2 \bmod 19 = 22^2 \bmod 19 = 13^2 \bmod 19 = 9$

$= 289 \bmod 19 = 9$

$p_6 = h(p_5) = (3\cdot 9+4)^2 \bmod 19 = 31^2 \bmod 19 = 12^2 \bmod 19 = 11$

initial record is $(A, N=6, 11)$

Q13. (4 points). What is electronic cash money? How it is represented? How it is validated? How its denomination is defined? What measure are used to protect from the electronic cash repeated spending?

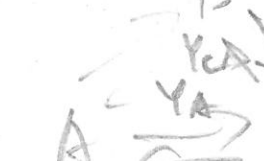
Electronic cash money is a money used as usual cash but having electronic representation. It is represented as encrypted with a private key of a bank serial number. It is validated by decryption the serial number with the public key of a bank and checking that a validation predicate on it returns true. Denomination is defined by pair of keys, private, public, used for its encryption / decryption. To withstand repeated money spending, the bank maintains a database with already spent serial numbers and a new serial is checked versus already spent ones.

Q14. (8 points). Explain how Biswas group key exchange protocol works on an example of three group members. Provide an example of such group key exchange. Show your calculations. Give necessary explanations.

Let $n = 3 \rightarrow$ 2 members + controller A, B

Each participant specifies his secret $X_A = 2, X_B = 3, X_C = 4$

g value is specified as a generator $G = (p)$ Let $p = 7$; $g = 3$



$g^1 = 3$ $g^2 = 2$ $g^3 = 6$ $g^4 = 4$ $g^5 = 5$

$g^6 = 1 \mod 7$

$Y_A = 3^{X_A} = 3^2 = 2$, $Y_B = 3^3 = 6$ $Y_C = 3^4 = 4$

$K_A = 3^{X_A X_C} = 2^4 = 2$ $K_B = 3^{X_B X_C} = 6^4 = 1$

$K = 3^{K_A K_B} = 3^{2 \cdot 1} = 2 \leftarrow$ calculated by C

C sends to A $3^{k_B} = 3$, A calculates
$k = 3^{k_A} = 3^2 = 2$
C send to B $3^{k_A} = 3^2 = 2$, B
calculates $k = 2^1 = 2$
Thus, all three participants share
a key $k = 2$.

Q15. (5 points). Explain how Address Resolution Protocol (ARP) works. Explain ARP Spoofing.

A requesting computer broadcast a request message "IP mac?" asking for a mac address of a specified IP address. The holder of the IP specified replies by a reply message "For IP MAC is that". On getting a reply message, the requester records the pair (IP, MAC) in its ARP cache.

ARP spoofing exploits a vulnerability of the protocol, that even without request, on comply a reply message, a computer changes its cache thus associating IP address it needs with a wrong MAC address.