Technische Universität Braunschweig

IDA INSTITUT FÜR DATENTECHNIK UND KOMMUNIKATIONS-NETZE

Cryptology System Design Fundamentals

Grundlagen des kryptographischen Systementwurfs

Module ID: ET-IDA-057, ET-IDA-110

Final Examination

Design-Problems Section: Open book examination part

V9-adi

Prof. W. Adi

Date : 22.07.2021
Duration : 90 Minutes. 75% of the evaluation score

Please write your answer on the same question sheet.
Bitte schreiben Sie die Lösungen auf die Aufgabenblätter.

Vorname .....

Nachname .....

Matrikel-Nr. .....

Fachrichtung: .....

Sample Solution

1

Max 75% of the marks

	Marks:
Problem 1	22
Problem 2	7
Problem 3	26
Problem 4	25
Total	80

2

Problem 1: RSA Public Key System (22 P)

A RSA cryptosystem with two users A and B having the following secret prime number pairs: for user A: 29 and 13 and for user B: 37 and 7.

1. **Find out the adequate public key of user A from the following list of integers: [48, 121, 168] giving the reason for your choice. Compute the corresponding secret key of user A.**
2. **Find out the adequate public key of user B from the following list of integers: [36, 49, 108] giving the reason for your choice. Compute the corresponding secret key of user B.**
3. **How many distinct public keys are possible for each user?**
4. **User A received the cryptogram $Y_B = 97$ from user B. Decipher the cryptogram Y_B on user A's side to get the original data M.**
5. **(a) User A computes the digest $H(M) = M^2 \bmod N_A$. A then signs the resulting digest H to generate his signature S_A.**
   (b) Compute S_A.
6. **Verify A's signature S_A on side B.**
7. **Which range of data values for M would operate adequately for enciphering M for communication between user A and others. Why?**
8. **(a) Why is it generally not possible for an adversary to reveal M from H(M)? (b) For which range of M can an attacker reveal the Message M by observing Y_B and S_A? State the necessary computations to reveal M.**

3

Solution Problem 1:

1. What is the adequate public key of user A from the following list of integers: [48, 121, 168], why?

$N_A = 29 \times 13 = 377$
$\varphi(N_A) = (29-1)(13-1-1) = 28 \times 12 = 336$
Since: gcd [E_A, $\varphi(N_A)$] = 1
$\Rightarrow$ Select, $E_A = 121$ **3**

Compute the corresponding secret key of user A:

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE = B2	GCD	
336	121	1	0	0	1	2	94			
121	94	0	1	1	-2	1	27			
94	27	1	-1	-2	3	3	13			
27	13	-1	4	7	-11	2	1	FALSE		
13	1	4	-9	-11	25	13	0	INVERSE=	25	GCD= 1

$D_A = 121^{-1} \bmod 336 = 25$ **2**

2. What is the adequate public key of user B from the following list of integers: [36, 49, 108], why?

$N_B = 37 \times 7 = 259$
$\varphi(N_B) = (37-1)(7-1) = 36 \times 6 = 216$
gcd (E_B, $\varphi(N_B)$) = 1
$\Rightarrow$ Select, $E_B = 49$ **3**

Compute the corresponding secret key of user B.

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE = B2	GCD	
216	49	1	0	0	1	4	20			
49	20	0	1	1	-4	2	9			
20	9	1	-2	-4	9	2	2			
9	2	-2	5	9	-22	4	1	FALSE		
2	1	5	-22	-22	97	2	0	INVERSE=	97	GCD= 1

$D_B = 49^{-1} \bmod 216 = 97$ **2**

4

Solution Problem 1:

3. How many distinct public keys are possible for each user? **2**

# of keys for user A = $\varphi[\varphi(N_A)] = \varphi(336) = 2^4 \times 3 \times 7 \times (1-1/2)(1-1/3)(1-1/7) =$ **96 keys**, $336 = 2^4 \times 3 \times 7$

# of keys for user B = $\varphi[\varphi(N_B)] = \varphi(216) = 2^3 \times 3^3 \times (1-1/2)(1-1/3) =$ **72 keys**, $216 = 2^3 \times 3^3$

4. User A received the cryptogram $Y_B = 79$ from user B. Decipher the cryptogram Y_B on user A's side to get the original data M.

$$M = (Y_B)^{D_A} \bmod N_A$$
$$M = (97)^{25} \bmod 377 = 201$$ **2**

5. (a) User A computes the digest $H(M) = M^2 \bmod N_A$.

$$H = M^2 \bmod N_A = 2012 \bmod 377 = 62$$ **2**

(b) User A signs the resulting digest h to generate his signature S_A.

$$S_A = (H(M))^{D_A} \bmod N_A$$
$$S_A = (62)^{25} \bmod 377 = 179$$ **2**

6. Verify A's signature S_A on the side of B:

B computes the digest: $H = (S_A)^{E_A} \bmod N_A = (179)^{121} \bmod 377 = 62$

Verification : $H = M^2 \bmod N_A = 2012 \bmod 377 = 62$

Comparsion **2**

5

Cont. Solution Problem 1: **2**

7. Which range of data values for M would operate adequately for enciphering M for communication between user A and others. Why?

Range from 0 to $N_A - 1 = 377 - 1 = 376$. These are the only elements which can be represented in Z_{377}

8. (a) Why is it generally not possible for an adversary to reveal M from H(M)? (b) For which range of M can an attacker reveal the Message M by observing Y_B and S_A? State the necessary computations to reveal M.

(a) As H(M) = $M^2 \bmod N_A$, Computing $M = \sqrt{M^2 \bmod N_A}$ is not possible as the factorization of N_A is not feasible according to the state of the art (Rabin Lock: square root computation in a ring is equivalent to factorization)..

(b) If $M < \sqrt{N_A}$, in that case, the hash value H(M)= $M^2 \bmod N_A = M^2$ (As $M^2 < N_A$). The adversary can get $H(M) = (S_A)^{E_A} \bmod N_A = M^2$, Computing the square root of M^2 in this case is possible (without modulus). That is: $\sqrt{M^2} = \pm M'$, We have only two answers **M = M' or M = N_A – M'**

The correct **M' =M** is the one which fulfils $Y_B = (M')^{E_A} \bmod N_A$

Example: for M=15 < $\sqrt{377}$, $Y_B = (M)^{E_A} \bmod N_A = (15)^{121} \bmod 377 =$ **171**

$S_A = (H(M))^{D_A} \bmod N_A = S_A = (225)^{25} \bmod 377 =$ **238**

Adversary Computes: $M^2 = H = (S_A)^{E_A} \bmod N_A = (238)^{121} \bmod 377 = 225$

$\Rightarrow$ M'=$\sqrt{225} = \pm 15$, **M' = 15** or **M' = 377-15= 362**

Check: choice M' = 15, yields $(M)^{E_A} \bmod N_A = (15)^{121} \bmod 377 =$ **171**$= Y_B$, **=> Correct choice** or M'= 362 => $(362)^{121} \bmod 377 =$ **206** $\neq Y_B$ (which do not match the sent Y_B) **=> Not correct!**

6

Solution Problem 2: Arithmetic in GF(2^6) (7 P)

1. Compute the multiplicative inverse of $x^4 + x^3 + x^2 + x$ modulo $P(x) = x^6 + x^5 + x^4 + x^2 + 1$
2. Verify your result.

Solution:

1. Multiplicative inverse computation

$B_2 = B_1 - q\,B_2$

$P_1(x)$	$P_2(x)$	$B_1(x)$	$B_2(x)$	$Q(x)$	$R(x)$
$x^6 + x^5 + x^4 + x^2 + 1$	$x^4 + x^3 + x^2 + x$	0	1	x^2	$x^3 - x^2 + 1$
$x^4 + x^3 + x^2 + x$	$x^3 + x^2 + 1$	1	x^2	x	x^2
$x^3 + x^2 + 1$	x^2	x^2	$x^3 + 1$	$x + 1$	1
x^2	1	$x^3 + 1$	$x^4 + x^3 + x^2 + x + 1$	x^2	0

2. Result verification

$(x^4 + x^3 + x^2 + x + 1)(x^4 + x^3 + x^2 + x) = (x^4 + x^3 + x^2 + x)^2 + x^4 + x^3 + x^2 + x$
$= x^8 + x^6 + x^4 + x^6 + x^4 + x^3 + x^4 + x^3 + x^2 + x$
$= x^8 + x^4 + x^2 + x$
$= 1$

$P(x) = x^6 + x^5 + x^4 + x^2 + 1$
$\Rightarrow x^6 = x^5 + x^4 + x^2 + 1$
$\Rightarrow x^7 = x^6 + x^5 + x^3 + x$
$= x^5 + x^4 + x^2 + 1 + x^5 + x^3 + x$
$= x^4 + x^3 + x^2 + x + 1$
$\Rightarrow x^8 = x^5 + x^4 + x^3 + x^2 + 1$

$x^4 + x^3 + x^2 + x + 1 \;|\; x^3 + x^2 + 1$; $x^4 + x^3 + x$; x^2 ; x

$x^3 + x^2 + 1 \;|\; x^2$; x^3 ; $x^2 + 1$; x

$x^2 + 1 \;|\; x^2$; x^2 ; 1 ; 1

Page 7

7

Problem 3: EL-Gamal Cryptosystem over GF(2^6) (26 P)

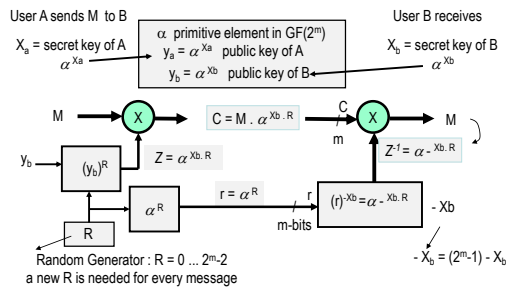
Set up ElGamal public-key system over GF(2^6) as in (Fig. 1).
The used field modulus is an irreducible primitive polynomial P(x).
The secret keys for users A and B are 19 and 7 respectively.

1. Which multiplicative orders are possible for elements in GF(2^6)? Why?
2. (a) Which is a primitive element in GF(2^6): x^5 or x^9 to be used as a public directory element α ? Why?
   (b) Compute the number of primitive elements in GF(2^6)?
3. Compute the public keys of user A and user B for the selected α .
4. (a) Send the message $M = \alpha^2$ from user A to B and use the random value R = 31 for this message.
   (b) Compute C and r.
5. Decrypt the cryptogram C to receive the message M on the side of user B.

Page 8

8

Fig.1 ElGamal Secrecy-System (1985)



Notice: The scheme applies similarly over GF(2^m) with α as a primitive element in that field.

Page 9

9

Solution Problem 3:

1. Which multiplicative orders are possible for elements in GF(2^6)? Why?

The possible orders are the divisors of $2^6 - 1 = 63$ → 1, 3, 7, 9, 21 and 63 (2)

2. (a) Which one is a primitive element in GF(2^6): x^5 or x^9 ? Why?

P(x) is primitive polynomial → x is primitive → Ord(x) = 63 which is the highest possible multiplicative order.

For $\alpha = x^5$:

$$Ord(\alpha) = Ord(x^5) = \frac{Ord(x)}{\gcd(Ord(x),5)} = \frac{63}{\gcd(63,5)} = 63 = \text{highest possible multiplicative order.}$$ (2)

For $\alpha = x^9$

$$Ord(\alpha) = Ord(x^5) = \frac{Ord(x)}{\gcd(Ord(x),9)} = \frac{63}{\gcd(63,9)} = \frac{63}{9} = 7 \neq \text{highest possible multiplicative order.}$$ (2)

$\Rightarrow \alpha = x^5$ is the primitive element (2)

(b) Compute the number of primitive elements in GF(2^6)?

The number of primitive elements is the number of the elements that have an order which is equal to the highest possible order which is 63
$\varphi(63) = \varphi(3^2 x 7) = 3^2 x 7 \times (1-1/3) \times (1-1/7) = 3x\,2\,x\,6 =$ **36** (2)

3. Compute the public keys of user A and user B.

User B (2)	User A (2)
Secret Key: $X_A = 19$	Secret Key: $X_B = 7$
Public Key: $Y_A = \alpha^{X_A} = (x^5)^{19} = x^{95 \bmod 63} = x^{32}$	Public Key: $Y_B = \alpha^{X_B} = (x^5)^7 = x^{35}$

Page 10

10

Solution Problem 3:

4. (a) Send the message $M = \alpha^2$ from user A to B using the random value R = 31 for this message.

$M = \alpha^2 = (x^5)^2 = x^{10}$ (2)
$Z = (Y_B)^R = (x^{35})^{31} = x^{1085 \bmod 63} = x^{14}$ (2)

(b) Compute C and r.

$C = M * Z = x^{10} * x^{14} = x^{24}$ (2)
$r = \alpha^R = (x^5)^{31} = x^{155 \bmod 63} = x^{29}$ (2)

5. Decrypt the cryptogram C to receive the message M on the side of user B.

$-X_B = (2^m - 1) - X_B = (2^6 - 1) - 7 = 56$ (2)
$Z^{-1} = r^{-X_B} = (x^{29})^{-7} = x^{-203 \bmod 63} = x^{49}$ (2)
$M = C * Z^{-1} = x^{24} * x^{49} = x^{73 \bmod 63} = x^{10}$ (2)

Page 11

11

Problem 4: Massey-Omura lock for Shamir's 3-Pass Protocol over GF(2^5) (25 P)

A Massey-Omura lock for Shamir's 3-Pass Protocol over GF(2^5) using the irreducible polynomial $p(x) = x^5 + x^2 + 1$ is used as a field modulus.

1. Compute the multiplicative order of x.
2. Compute the element x^{20} and x^{40} in binary format with minimum number of steps.
3. The secret key for users A and B are 23 and 13 respectively.
   A message $M = x^{21}$ is sent from A to B.
   Compute all the exchanged 3-pass messages as powers of x with the smallest possible power of x.
4. Compute the number of possible distinct secret keys for each user.
5. Compute the maximum number of simple exponentiation search cycles required to break the cipher by a known clear text–cipher text attack? (technical reasons are required!)

Page 12

12

Solution Problem 4:

A Massey-Omura lock for Shamir's 3-Pass Protocol over GF(2^5)
using the irreducible polynomial $p(x) = x^5 + x^2 + 1$ is used as a field modulus

1. **Compute the multiplicative order of x .**

Possible multiplicative orders are the divisors of $2^5 - 1 = 32-1=31$; 2
Divisors of 31 are: 1, 31

$x^1 \neq 1$, => multiplicative order of x is 31

2. **Compute the elements: x^{20} and x^{40} with minimum number of steps**

$p(x)= x^5 + x^2 + 1$
$\Rightarrow x^5 = x^2 + 1$ 2

$\Rightarrow x^6 = x^3+x$
$\Rightarrow x^7= x^4+x^2$
$\Rightarrow x^8= x^5+x^3 = x^3 + x^2 + 1$

2 $x^{20} = (x^5)^4 = (x^2 + 1)^4 = x^8 + 1 = x^3 + x^2 = 01100$

2 $x^{40} = (x^{20})^2 = (x^3 + x^2)^2 = x^6 + x^4 = x^3+x+ x^4 = 11010$

13

Solution Problem 4:

3. **The secret key for users A and B are 23 and 13 respectively.**
A message $M = x^{21}$ is sent from A to B.
Compute all the exchanged 3-pass messages as powers of x with the smallest possible power of x.

Keys of the user A
$E_a = 23$

2 $D_a = E_a^{-1}$
$= 23^{-1} \bmod 31$
$= 31-4= 27$

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE = B2		GCD	
31	23	1	0	0	1	1	8				
23	8	0	1	1	-1	2	7				
8	7	1	-2	-1	3	1	1				
7	1	-2	3	3	-4	7	0	INVERSE=	-4	GCD=	1

2 **Keys for user B**
$E_b = 13$

$D_b = E_b^{-1}$
$=13^{-1} \bmod 31$
=12

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE = B2		GCD	
31	13	1	0	0	1	2	5				
13	5	0	1	1	-2	2	3				
5	3	1	-2	-2	5	1	2				
3	2	-2	3	5	-7	1	1				
2	1	3	-5	-7	12	2	0	INVERSE=	12	GCD=	1

14

Solution Problem 4:

Keys of the user A
$E_a = 23, D_a = 27$

Keys for user B
$E_b = 13, D_b = 12$

1

Arithmetic in GF(2^5)

User A **User B**

$M = x^{21}$ 1 x^{18} $x^{18.13 \bmod 31} = x^{234 \bmod 31} = x^{17}$

$(x^{21})^{23} = x^{21.23 \bmod 31} = x^{483 \bmod 31} = x^{18}$ 2 2

2 x^{17}

$(x^{17})^{27}$ 3 x^{25} $(x^{25})^{12} = M$

$x^{17x27 \bmod 31} = x^{459 \bmod 31} = x^{25}$ $(x^{25})^{12 \bmod 31} = x^{21} = M$

2 2

4. **Compute the number of possible distinct secret keys for each user**

# of keys for each user is φ (31) = 31-1 = 30 2

15

5. **Compute the maximum number of simple exponentiation search cycles required to break the cipher by a known clear text–cipher text attack? (technical reasons are required!)** 2

A known clear text-cipher text
$\Rightarrow$ known M and known cryptogram $y = M^{Ea}$
$\Rightarrow$ The attacker needs to run a program that searches for $t = E_a$ which happens when $M^t = y$
The order of any $M \neq 0$ is 31, as 31 is a prime number. Possible E_a values are 1 to 31.
that is the search for E_a starts by M^1 M^2 .... Up to M^{30}
Since the # of usable keys for each user is 30
$\Rightarrow$ the attacker needs to check a maximum of 30 possible values of E_a
$\Rightarrow$ 30 is the number of the possible exponenetiation search cycles required.

16