Technische Universität Braunschweig

IDA Institut für Datentechnik und Kommunikationsnetze

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

Prof. W. Adi

Date : 06.03.2015
Duration : 120 Minutes. 70% of the evaluation score

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

Sample Solution

Vorname ....
Nachname ....
Matrikel-Nr. ....
Fachrichtung: ....

05.04.2021, V11

1

Max 70% marks

	Marks:
Problem 1	
Problem 2	
Problem 3	
Problem 4	
Problem 5	
Problem 6	
Optional	
Total	

2

P1: **(15 P)**

A RSA cryptosystem with two users A and B having the following secret prime number pairs: for user A: 53 and 17 and for user B: 41 and 19

1. **Find out the adequate public key of user A from the following list of integers: [35, 26, 48] 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: [125,1024,31] giving the reason for your choice. Compute the corresponding secret key of user B.**
3. **How many public keys are possible for each user?**
4. **User A encrypts the message M=9, and send the resulting cryptogram Y_{AB} to B. User A then signs the cryptogram Y_{AB} and generates the signature S_{AB} . Compute Y_{AB} and S_{AB}.**
5. **Decipher the cryptogram Y_{AB} on user B's site and verify the Signature S_{AB}.**
6. **User B signs the received message M and sends his signature S_{BA} back to A. Compute the signature S_{BA}.**

3

Solution:

1. **Find out the adequate public key of user A from the following list of integers: [35, 26, 48] giving the reason for your choice. Compute the corresponding secret key of user A.**

N_A = 53 x 17 = 901, φ (N_A) = (53-1)(17-1) = 832
gcd [E_A, φ (N_A)] = 1 => select 35 as gcd (832,35) = 1
E_A = 35
D_A = -309 mod 832 = 523 (see computation below)

2

$D_A = 35^{-1}$ mod 832 = -309 + 832 = 523

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE		GCD	
832	35	1	0	0	1	23	27				
35	27	0	1	1	-23	1	8				
27	8	1	-1	-23	24	3	3				
8	3	-1	4	24	-95	2	2				
3	2	4	-9	-95	214	1	1				
2	1	-9	13	214	-309	2	0	INVERSE=	-309	GCD=	1

2. **Find out the adequate public key of user B from the following list of integers: [125,1024,31] giving the reason for your choice. Compute the corresponding secret key of user B.**

N_B = 41 x 19 = 779 , φ (N_B) = (41-1)(19-1) = 720
gcd (E_B, φ (N_B)] =1 => select 31 as gcd (720,31) = 1
E_B = 31
D_B = -209 mod 720 = 511 (see computation below)

2

$D_B = 31^{-1}$ mod 720 = -209 + 720 = 511

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE		GCD	
720	31	1	0	0	1	23	7				
31	7	0	1	1	-23	4	3				
7	3	1	-4	-23	93	2	1				
3	1	-4	9	93	-209	3	0	INVERSE=	-209	GCD=	1

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

\# of keys for user A = φ [φ (N_A)] = φ (832) = φ (2^6.13)= 832(1 -1/2) (1 – 1/13) = 384 keys
\# of keys for user B = φ [φ (N_B)] = φ (720) = φ (2^4 . 3^2 . 5)= 720(1 -1/2) (1 -1/3) (1 -1/5) = 192 keys

2

4

4. **User A encrypts the message M=9, and send the resulting cryptogram Y_{AB} to B. User A then signs the cryptogram Y_{AB} and generates the signature S_{AB} . Compute Y_{AB} and S_{AB}.**

$$Y_{AB} = (M)^{E_B} \bmod N_B$$
$$Y_{AB} = (9)^{31} \ mod\ 779$$
$$Y_{AB} = 196$$

$$S_{AB} = (Y_{AB})^{D_A} \bmod N_A$$
$$S_{AB} = (196)^{523} \bmod 901 = 780$$

3

5. **Decipher the cryptogram Y_{AB} on user B's site and verify the Signature S_{AB}.**

Decryption:

$$M = (Y_{AB})^{D_B} \bmod N_B$$
$$M = (9^{31})^{511} \bmod 779$$
$$\mathrm{M} = 9^{15841 \bmod 720} \bmod 779 = 9$$

Verification:

check if: $(S_{AB})^{E_A} \bmod N_A = Y_{AB} \bmod N_A$

$(780)^{35} \bmod 901 = ... = 196 = Y_{AB}$
=> **signature is authentic!**

4

6. **User B signs the received message M and sends his signature S_{BA} back to A. Compute the signature S_{BA}.**

2

$$S_{BA} = (M)^{D_B} \bmod N_B$$
$$S_{BA} = (9)^{511} \bmod 779 = 688$$

5

P2: **(9 P)**

(b) A block cipher with a key length of 256 bits is encrypting a clear text with a block size of 1000 bit having a clear text entropy of 900 bits.

1. **Compute the unicity distance of the cipher n_u**
2. **Compute the new unicity distance of the cipher if 500 random bits are appended to each clear text block**
3. **Is the cipher theoretically breakable after this modification if the attacker can observe 2700 cipher text bits? Why?**

Solution:

K= 256 Bits, H(x)=900 Bits, N= 1000 Bits, r = ?

1. Unicity distance n_u = K/r

   As r = [N – H(x)] / N
   => r = (1000 – 900) / 1000 = 0.1 => **n_u** = K/r = 256/0.1 = **2560 Bits**

   4

2. n'_u = [(L + N) / N] · n_u

   3

   n'_u = [(500 + 1000) / 1000] · 2560

   n'_u = 3840 Bits

3. The number of observed cipher text bits is only 2700 bits and is **less** than the unicity distance (3840 bits). Therefore, the cipher is theoretically **not** possible to break

   2

6

P3: Compute the multiplicative inverse of $(011000000)_2$ modulo $P(x) = (110110001)_2$ and verify your result! **(7 P)**

Solution:

Extended gcd Algorithm:

B2 = B1 – q B2

$\boxed{5}$

$P_1(x)$	$P_2(x)$	B1(x)	B2(x)	Q(x)	R(x)
$x^8 + x^7 + x^5 + x^4 + 1$	$x^7 + x^6$	0	1	x	$x^5 + x^4 + 1$
$x^7 + x^6$	$x^5 + x^4 + 1$	1	x	x^2	x^2
$x^5 + x^4 + 1$	x^2	x	x^3+1	$x^3 + x^2$	1
x^2	1	x^3+1	$x^6+x^5+x^3+x^2+x$	x^2	0

Verification: $\boxed{2}$

$\Rightarrow (x^6+x^5+x^3+x^2+x) \equiv (x^7 + x^6)^{-1}$ modulo $(x^8 + x^7 + x^5 + x^4 + 1)$

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

$= x^{13} + \cancel{x^{12}} + x^{10} + \cancel{x^9} + \cancel{x^8} + \cancel{x^{12}} + x^{11} + \cancel{x^9} + \cancel{x^8} + x^7$

$= x^{13} + x^{11} + x^{10} + x^7$

$= \cancel{x^7} + \cancel{x^5} + \cancel{x^4} + \cancel{x^3} + \cancel{x^5} + \cancel{x^3} + \cancel{x^2} + \cancel{x} + \cancel{x^4} + 1 + \cancel{x} + \cancel{x^2} + \cancel{x^7}$

$= 1$

$x^8 = x^7 + x^5 + x^4 + 1$

$x^9 = x^8 + x^6 + x^5 + x = x^7 + x^5 + x^4 + 1 + x^6 + x^5 + x$

$= x^7 + x^4 + 1 + x^6 + x$

$x^{10} = x^8 + x^5 + x + x^7 + x^2 = x^7 + x^5 + x^4 + 1 + x^5 + x + x^7 + x^2$

$= x^4 + 1 + x + x^2$

$x^{11} = x^5 + x^3 + x^2 + x$

$x^{12} = x^6 + x^4 + x^3 + x^2$

$x^{13} = x^7 + x^5 + x^4 + x^3$

Page 7

7

P4: A Diffie-Hellman (DH) public key exchange system uses $GF(2^6)$ deploying the irreducible polynomial $p(x) = x^6 + x^3 + 1$. **(21 P)**

1. For $\beta = x$, compute β^i for i = 1 to 10. What is the multiplicative order of x? $\boxed{2}$
2. Which multiplicative orders are possible for elements in $GF(2^6)$? $\boxed{2}$
3. Prove that the element $\delta = 1+x = 000011$ is a primitive element. $\boxed{4}$
4. Compute the multiplicative order of δ^{14} $\boxed{2}$
5. Use the element δ as a public element in the above $GF(2^6)$ and compute the DH public keys Y_a and Y_b and the shared secret key Z_{AB} for users A and B having the secret keys $X_a=42$ und $X_b=14$. $\boxed{6}$
   compute the binary vectors for Y_a and Y_b and Z_{AB} by making use of the following : $\delta^7 = x^5 + x^2$, $\delta^{21} = 1 + x^3$,
6. What is the probability of getting an element with order 21 if the element is picked up randomly from $GF(2^6)$?. $\boxed{2}$
7. For any element α from $GF(2^6)$, compute t for which $\alpha^{-1} = \alpha^t$ ·
   Compute then x^{-1} mod p(x) using that result. (Hint make use of the results in 1) $\boxed{3}$
   Verify your result.

Page 8

8

Solution:

1. For $\beta = x$, compute β^i for i = 1 to 10. What is the multiplicative order of x?

$P(x) = x^6 + x^3 + 1 = 0 \quad \Rightarrow \quad x^6 = x^3 + 1$

$x^1 = x$
$x^2 = x^2$
$x^3 = x^3$
$x^4 = x^4$
$x^5 = x^5$
$x^6 = x^3 + 1$
$x^7 = x^4 + x$
$x^8 = x^5 + x^2$
$x^9 = x^6 + x^3 = x^3 + x^3 + 1 = 1$
$x^{10} = x$
$ord(x) = 9$

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

Possible orders are the divisors of $2^6 - 1 = 63$
Divisors of 63 are: 1,3,7,9,21 and 63

3. Prove that the element $\delta = 1+x = 000011$ is a primitive element.

$(x+1)^1 = x+1 \neq 1$

$(x+1)^3 = (x+1)^2 \cdot (x+1) = (x^2+1).(x+1) = x^3+x^2+x+1 \neq 1$

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

$= x^4+x+x^5+x^3+x+x^3+1+x^4+x^2+1 = x^5+x^2 \neq 1$

$(x+1)^9 = (x+1)^7 \cdot (x+1)^2 = (x^5+x^2) \cdot (x^2+1) = x^7+x^4+x^5+x^2 = x^4+x+x^4+x^5+x^2 = x^5+x^2+x \neq 1$

$(x+1)^{21} = ((x+1)^7)^3 = (x^5+x^2)^3 = (x^5+x^2)^2 \cdot (x^5+x^2) = (x^{10}+x^4) \cdot (x^5+x^2) = (x+x^4) \cdot (x^5+x^2)$

$= \cancel{x^6}+x^3+x^9+\cancel{x^6} = x^3+1 \neq 1 \rightarrow ord(x+1) = 63$

$X^6 = x^3 + 1$
$X^7 = x^4 + x$
$X^8 = x^5 + x^2$
$x^9 = x^6 + x^3$
$= x^3 + x^3 + 1 = 1$
$x^{10} = x$

Page 9

9

4. Compute the multiplicative order of δ^{14}

$$ord(\delta^{14}) = \frac{ord(\delta)}{\gcd(ord(\delta), i)} = \frac{63}{\gcd(63,14)} = \frac{63}{7} = 9$$

5. Use the element δ as a public element in the above $GF(2^6)$ and compute the DH public keys Y_a and Y_b and the shared secret key Z_{AB} for users A and B having the secret keys $X_a=42$ und $X_b=14$.

compute the binary vectors for Y_a and Y_b and Z_{AB} by making use of the following : $\delta = x+1$, $\delta^7 = x^5 + x^2$, $\delta^{21} = 1 + x^3$,

User A:
$X_a = 42$,
$Y_a = \delta^{42} = (x+1)^{42} \bmod (x^6+x^3+1)$
$= ((x+1)^{21})^2 = (\delta^{21})^2 = (x^3+1)^2$
$= x^6+1 = x^3+1 + 1 = x^3$
$= 001000$

Public directory $GF(2^6)$
$\delta = x+1$, $P(x) = x^6 + x^3 + 1$
$Y_a = x^3 = 001000$
$Y_b = x^4+x = 010010$

User B:
$X_b = 14$,
$Y_b = \delta^{14} = (\delta^7)^2$
$= (x^5+x^2)^2$
$= x^{10}+x^4 = x^4 + x$
$= 010010$

Common secret key for users A and B
$Z_{ab} = \delta^{42.14 \bmod 63} = (x+1)^{42 \,.\, 14 \bmod 63} = (x+1)^{21} = x^3+1$
$Z_{ab} = x^3 + 1 = 001001$

6. What is the probability of getting an element with order 21 if the element is picked up randomly from $GF(2^6)$?.

# of all non-zero elements : $2^6 - 1 = 63$
# of elements with order 21: $\varphi(21) = \varphi(7 \times 3) = (7-1).(3-1) = 6 \,.\, 2 = 12$
Probabilty of (element's order=21) = (12 / 63) . 100 = 19.05 %

Page 10

10

7. For any element α from $GF(2^6)$, compute t for which $\alpha^{-1} = \alpha^t$ ·
   Compute then x^{-1} mod p(x) using that result. (Hint make use of the results in 1)
   Verify your result.

For any element t, $\alpha^{-1 \text{ mode } 63} = \alpha^{-1+63} = \alpha^{62} = \alpha^t \rightarrow t = 62$

$x^{-1} = x^{62} = (x^9)^6 . x^8 = (1)^6 . x^8 = x^8$

$x^{-1} = x^8 = x^5 + x^2$

Verification:

$x \,.\, x^{-1} = x \,.\, x^8 = x^9 = 1$ (see 1)

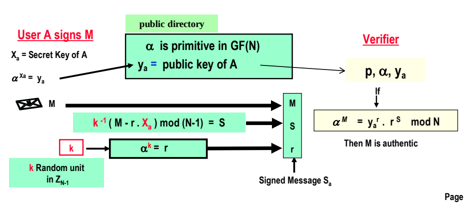
Page 11

11

(15 P)

P5: El-Gamal crypto system is set up using the prime number $N = 2 \cdot 281 + 1 = 563$ generated by applying Pocklington's Theorem, where q=281 is a prime.

1. Prove that N is a prime according to Pocklington's Theorem. $\boxed{3}$
2. Find a primitive element in GF(563) and use it as a public element in ElGamal public key system (show all necessary computations). $\boxed{2}$
3. User A encrypts the message M=33 and send it to user B who has the secret key $X_b= 70$ by using the random number R=17. Compute B's public key Y_b and the encrypted message C_a and r. $\boxed{5}$
4. Decrypt the cryptogram C_a on the receiver side B showing all necessary computations therefore. $\boxed{2}$
5. Let user A having the secret key $X_a= 133$ compute his Signature S_a according to ElGamal signature scheme shown below for the same message M=33 . Select one adequate k from the following list (k = 22,270,89). $\boxed{3}$



Page 12

12

Solution:

1. Prove that N is a prime according to Pocklington's Theorem.

N = R . F + 1= **2 · 281 + 1 = 563**, F = 281 is a prime, and R = 2. Is N=563 a prime? (1)

Choose a=2.

Proof: 1. gcd ($a^{(N-1)/pj}$ –1 , N) = gcd ($a^{(563-1)/281}$ –1 , N) = gcd (2^2–1 , 563) = gcd (3 , 563) = 1 is true

2. a^{N-1} = 1 (mod N) ⇔ 2^{562} = 1 (mod 563) is true

3. F > √N
281 >√563= 23.7 => 281> 23.7 is true
As all conditions 1, 2 and 3 are all true ⇒ 563 is for sure a prime number

2. Find a primitive element in GF(563) and use it as a public element in ElGamal public key system (show all necessary computations).

Possible orders are the divisors of (563 -1) = 562
Divisors of 562 are: 1,2,281 and 562 as can be seen from (1)

Checking if the element 2 is primitive
2^1 mod 563 ≠ 1 ,
2^2 mod563 ≠ 1 ,
2^{281} mod563 = 562 ≠ 1
⇒ Ord (2) = 562 ⇒ α = 2 is primitive element

3. User A encrypts the message M=33 and send it to user B who has the secret key X_b= 70 by using the random number R=17. Compute B's public key Y_b and the encrypted message C_a and r.

Encryption:

User B.
X_b = 70
$Y_b = \alpha^{X_b}$ mod p= 2^{70} mod 563 = 445

Public directory
α = 2 , GF(563)
$Y_B = 2^{70}$ mod 563 = 445

User A.
M = 33

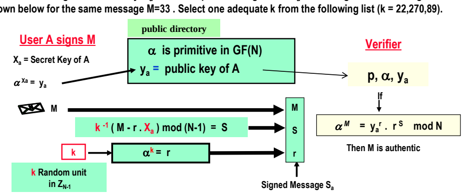
r = $\alpha^R = 2^{17}$ mod 563 = 456
$C_a = M . Y_B^R = 33 . (2^{70})^{17}$ mod 563 = 33. 63 = 390

4. Decrypt the cryptogram C_a on the receiver side B showing all necessary computations, therefore.

Decryption:

$Z^{-1} = (\alpha^R)^{-X_b} = r^{-X_b} = 456^{-70 \bmod 562}$ mod 563 = $(456^{-70+562})$mod 563 = 143
M = $C_a . Z^{-1}$ = 390 · 143 mod 563 = 33

5. Let user A having the secret key X_a= 133 compute his Signature S_a according to ElGamal signature scheme shown below for the same message M=33 . Select one adequate k from the following list (k = 22,270,89).



K has to be invertible mod N-1, N-1=562
gcd [k, N-1] = 1 => select 89 from the list (k = 22,270,89) . As gcd (562,89) = 1
K = 89 , 89^{-1} = -221 mod 562 = 341 (see table below)
r = $\alpha^k = 2^{89}$ mod 563 = 397
S = k^{-1} (M - r . X_a) mod (N-1)
= 89^{-1}(33- 397 . 133) mod 562
= 341 (33 – 52801) mod 562
= 341 . (-52768)mod 562
S = -17993888 mod 562 = -334 + 562 = 228

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE =		GCD	
562	89	1	0	0	1	6	28				
89	28	0	1	1	-6	3	5				
28	5	1	-3	-6	19	5	3				
5	3	-3	16	19	-101	1	2				
3	2	16	-19	-101	120	1	1				
2	1	-19	35	120	-221	2	0	INVERSE=	-221	GCD=	1

P6: **(11 P)**

A Massey-Omura lock for Shamir's 3-Pass Protocol over GF(2^8) using the irreducible polynomial p(x) = $x^8 + x^7 + x^3 + x + 1$ as a field modulus is set up.
(Hint: 2^8-1 = 3 · 5 · 17)

1. **Write p(x) in binary form and find out the multiplicative order of x (by using the list of binary irreducible polynomials).** 1,5
2. **Compute the powers of x in GF(2^8) (x^9 and x^{10}).** 1,5
3. **The secret key for users A and B are 7 and 13 respectively. A message M = x^8 is sent from A to B. Compute all the exchanged 3-pass messages as powers of x with smallest possible power of x.** 2
4. **Compute the number of possible secret keys in case that the sent clear text message M was only selected as a power of x. (that is M=x^i for some i).** 3
5. **What is the maximum number of exponentiation search cycles required to break a message of the form (M=x^i) ? Why?** 3

Solution:

1. **Write p(x) in binary form and find out the multiplicative order of x (by using the list of binary irreducible polynomials).**

The polynomial binary pattern is : p(x) = $x^8 + x^7 + x^3 + x + 1$ = **110001011**

e of p(x) is = 85 (see list of irreducible polynomials in the lecture slides)
⟶ order of x modulo p(x) is 85.
⟶ x^{85} =1

2. **Compute the powers of x in GF(2^8) (x^9 and x^{10}).**

p(x) = $x^8 + x^7 + x^3 + x + 1$ = 0
=> $x^8 = x^7 + x^3 + x + 1$
$x^9 = x^8 + x^4 + x^2 + x = (x^7 + x^3 + \cancel{x} + 1) + x^4 + x^2 + \cancel{x} = x^7 + x^3 + 1 + x^4 + x^2$
$x^{10} = x * x^9 = x *(x^7 + x^3 + 1 + x^4 + x^2) = x^8 + \cancel{x^4} + x + x^5 + x^3 = (x^7 + \cancel{x^3} + \cancel{x} + 1) + x^4 + \cancel{x} + x^5 + \cancel{x^3} = x^7 + 1 + x^4 + x^5$

3. **The secret key for users A and B are 7 and 13 respectively. A message M = x^8 is sent from A to B. Compute all the exchanged 3-pass messages as powers of x with smallest possible power of x.**

A
Ea=7 as gcd(2^8-1,7) = 1
Da = Ea^{-1} (mod 2^8 -1)
Da = 7^{-1} (mod 255)= **73**

Public directory :
GF(2^8), **polynomial** p(x) = $x^8 + x^7 + x^3 + x + 1$

B
Eb= 13 as gcd(2^8-1,13)=1
Db = Eb^{-1} (mod 2^8 -1)
Db = 13^{-1} (mod 255)= -98 = -98+255= **157**

As the order of x is 85, the modulus in the exponents of x is 85 !!!

M = x^8 $\xrightarrow{Y_1 = M^{Ea} = x^{8 \cdot 7} = x^{56}}$ **$Y_1 = x^{56}$**

$Y_2 = (Y_1)^{Eb}$
$Y_2 = (Y_1)^{Eb} = M^{Ea \cdot Eb \bmod p-1}$
$= x^{56 \cdot 13 \bmod 85} = x^{48}$

$\xleftarrow{Y_2 = x^{48}}$

$Y_3 = (Y_2)^{Da} = M^{Ea \cdot Eb \cdot Da \bmod p-1}$
$= x^{48 \cdot 73 \bmod 85} = x^{19}$

$\xrightarrow{Y_3 = x^{19}}$

$M = (Y_3)^{Db \bmod p-1} = (x^{19})^{157 \bmod 85}$
M = x^8

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE =		GCD	
255	7	1	0	0	1	#	3				
7	3	0	1	1	-36	2	1				
3	1	1	-2	-36	73	3	0	INVERSE=	73	GCD=	1

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE = B2		GCD	
255	13	1	0	0	1	19	8				
13	8	0	1	1	-19	1	5				
8	5	1	-1	-19	20	1	3				
5	3	-1	2	20	-39	1	2				
3	2	2	-3	-39	59	1	1				
2	1	-3	5	59	-98	2	0	INVERSE=	-98	GCD=	1

4. Compute the number of possible secret keys in case that the sent clear text message M was only selected as a power of x. (that is $M=x^i$ for some i).

If the attacker knows that the sent messages are powers of x, then the modulus in the exponent is 85 (85 is the order of x). The number of distinct messages is then only 85
The cryptographically significant keys are those usable for 85 as a modulus instead of 255.
The usable keys are those which are invertible modulo 85.
The number of such keys is $\varphi(85) = \varphi(5 \times 17) = (5-1).(17-1) = 4 \times 16 = 64$ keys.

5. What is the maximum number of exponentiation search cycles required to break a message of the form ($M=x^i$) ? Why?

As the maximum number of search cycles to compute the discrete logarithm is the maximum order involved in the terms to be attacked. The attacked term in that case is x^i.
The order of any element having the form (x^i) for any i is = 85/ gcd(85,i). The maximum value for the order is for i such that gcd(85,i) =1. That is the maximum order is 85 and the maximum number of simple search cycles to get the discrete logarithm is 85.
Breaking a system is reached if the secret key could be found for one encrypted message as Y_1 in this example.