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
V14-A 31.05.2023
Prof. W. Adi

Date : 16.03.2018
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: ....

06.04.2021 - v12

1

Max 70% marks

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

2

P1: **(25 P)**

A RSA cryptosystem with two users A and B having the following secret prime number pairs: for user A: 11 and 23 and for user B: 13 and 17

1. **Find out the adequate public key of user A from the following list of integers: [15, 87, 112] 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: [55,120,159] 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 B encrypts the message M=19, and send the resulting cryptogram Y_{BA} to A. User B then signs h= (M^2) mod N_A and generates the signature S_{BA} . Compute Y_{BA} and S_{BA}.**
5. **For which range of the values of M can an attacker compute M by observing S_{BA} ? Why?**
6. **Decipher the cryptogram Y_{BA} on user A's site and verify the Signature S_{BA}.**

3

Solution:

1. **Find out the adequate public key of user A from the following list of integers: [15, 87, 112] giving the reason for your choice. Compute the corresponding secret key of user A.**

N_A = 11 x 23 = 253, φ (N_A) = (11-1)(23-1) = 220
gcd [E_A, φ (N_A)] = 1 => select 87 as gcd (87,220) = 1
E_A = 87
D_A = 43 mod 220 = (see computation below)

3

$D_A = 87^{-1}$ mod 220 =43

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE		GCD	
220	87	1	0	0	1	2	46				
87	46	0	1	1	-2	1	41				
46	41	1	-1	-2	3	1	5				
41	5	-1	2	3	-5	8	1				
5	1	2	-17	-5	43	5	0	INVERSE=	43	GCD=	1

2.Find out the adequate public key of user B from the following list of integers: [55,120,159] giving the reason for your choice. Compute the corresponding secret key of user B.

3

N_B = 13 x 17 =221 , φ (N_B) = (13-1)(17-1) = 192
gcd (E_B, φ (N_B)] =1 => select 3 as gcd (55,192) = 1
E_B = 55
D_B = 7 mod 192 (see computation below)

$D_B = 55^{-1}$ mod 192 = 7

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE		GCD	
192	55	1	0	0	1	3	27				
55	27	0	1	1	-3	2	1				
27	1	1	-2	-3	7	27	0	INVERSE=	7	GCD=	1

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

# of keys for user A = φ [φ (N_A)] = φ (220) = φ (2^2 . 5. 11)= 220(1 -1/2).(1 – 1/5).(1 – 1/11) = 80 keys 4
# of keys for user B = φ [φ (N_B)] = φ (192) == φ (2^6 . 3)= 192(1 -1/2) (1 -1/3) = 64 keys

4

4. **User B encrypts the message M=19, and send the resulting cryptogram Y_{BA} to A. User B then signs h= (M^2)mod N_A and generates the signature S_{BA} . Compute Y_{BA} and S_{BA}. Can an attacker get M by observing S_{BA} . if yes how? If No, why?**

Encryption:
$Y_{BA} = (M)^{Ea} \bmod N_a = (19)^{87} \bmod 253 = 178$ 6

Sings:
$H(M) = h = (M^2 \bmod N_A) = 19^2 \bmod 253 = 108$
$S_{BA} = (h)^{Db} \bmod N_b = (108)^7 \bmod 221 = 82$

5

5. **For which range of values of M can an attacker compute M by observing S_{BA} ? Why?**

Computing M is passable if $M^2 < N_A$ in that case the square root is computable. As the modulus N_A would deliver the real M^2 and computing the square root is straight forward as the modulus is not involved.
If however, the modulus is involved, then computing the square root mod N_A is only possible if the factorization of N_A is known.

6. **Decipher the cryptogram Y_{BA} on user A's site and verify the Signature S_{BA}**

Decipher:
$M = (Y_{BA})^{Da} \bmod N_a = (178)^{43} \bmod 253 = 19$ 4

Verification if M is signed by B::
$h = (S_{BA})^{Eb} \bmod N_b = (82)^{55} \bmod 221 = 108$
Check if h=108 = M^2 mod N_a = 19^2 mod 253 = 108 is true. Therefore, Signature of B is authentic..

5

P2: DH over GF(2^5) **(28 P)**

A Diffie-Hellman (DH) public key exchange system uses GF(2^5) deploying the primitive Polynomial $P(x) = x^5 + x^2 + 1$ as field modulus.

1. **Compute the exponents of the element x = 000010 as x^i mod P(x) for i= 1 to 10 in binary form in GF(2^5).**
2. **Which multiplicative orders are possible for elements in GF(2^5)? Why? Compute the multiplicative order of the element $\beta = x^{15}$ and its binary vector.**
3. **Use the element β as a public element and compute the DH public keys Y_a and Y_b as binary vectors for users A and B having the secret keys X_a=13 und X_b=19.**
4. **Compute the polynomial and binary pattern for the shred key Z_{AB} of users A and B .**
5. **Setup the ElGamal cryptosystem and compute the cryptogram C_A as a binary vector for the message $M=x^{30}$ sent from A to B by using the same above DH setup and using a random R=11.**
6. **Decrypt C_A on B's side showing all necessary computations.**

6

Solution

1. Compute the exponents of the element $x = 000010$ as $x^i \bmod P(x)$ for i= 1 to 10 in binary form in $GF(2^5)$.

$P(x) = x^5 + x^2 + 1 = 0 \quad \Rightarrow \quad x^5 = x^2 + 1$

$x^1 = x = 00010$
$x^2 = x^2 = 00100$
$x^3 = x^3 = 01000$
$x^4 = x^4 = 10000$
$x^5 = x^2 + 1 = 00101$
$x^6 = x^3 + x = 01010$
$x^7 = x^4 + x^2 = 10100$
$x^8 = x^5 + x^3 = x^3 + x^2 + 1 = 01101$
$x^9 = x^4 + x^3 + x = 11010$
$x^{10} = x^5 + x^4 + x^2 = x^4 + \cancel{x^2} + \cancel{x^2} + 1 = 10001$

2. Which multiplicative orders are possible for elements in $GF(2^5)$? Why? Compute the multiplicative order of the element $\beta = x^{15}$ and its binary vector.

Possible orders are the divisors of $2^5-1 = 31$: that are: 1, 31. As $x^1 \neq 1 \Rightarrow Ord(x)=31$

As $\boxed{ord(\alpha^i) = \frac{ord(\alpha)}{\gcd[ord(\alpha), i]}}$ ⇨ $ord(\beta) = ord(x^{15}) = \frac{31}{\gcd[31,15]} = 31$

$\beta = x^{15} = x^{10} . x^5 = (x^4 + 1)(x^2 + 1) = x^6 + x^4 + x^2 + 1 = x^3 + x + x^4 + x^2 + 1 = x^4 + x^3 + x^2 + x + 1 = 11111$

3. Use the element β as a public element and compute the DH public keys Y_a and Y_b as binary vectors for users A and B having the secret keys $X_a=13$ und $X_b=19$.

User A:
$X_a = 13$,
$Y_a = \beta^{13} = (x^{15})^{13}$
$= x^{15.13 \bmod 31} = x^9$
$= x^4 + x^3 + x$

⇨ $Y_a = 11010$

$\boxed{2}$

Public directory $GF(2^5)$
$\beta = x^{15}$, $P(x) = x^5 + x^2 + 1$

$Y_a = 11010$

$Y_b = 01010$

User B:
$X_b = 19$,
$Y_b = \beta^{19} = (x^{15})^{19}$
$= x^{15.19 \bmod 31} = x^6$
$= x^3 + x$

⇨ $Y_b = 01010$

$\boxed{2}$

4. Compute the polynomial and binary pattern for the shred key Z_{AB} of users A and B . $\boxed{4}$

Common secret key for users A and B:
$Z_{ab} = ((x^{15})^{13})^{19} = x^{3705 \bmod 31} = x^{16} = x^{10} . x^6 = (x^4 + 1).(x^3 + x) = x^7 + x^5 + x^3 + x = x^4 + \cancel{x^2} + \cancel{x^2} + 1 + x^3 + x$

$\boxed{Z_{ab} = x^4 + x^3 + x + 1 = 11011}$

5. Setup the ElGamal cryptosystem and compute the cryptogram C_A as a binary vector for the message $M=x^{30}$ sent from A to B by using the same above DH setup and using a random R=11.

6. Decrypt C_A on B's side showing all necessary computations.

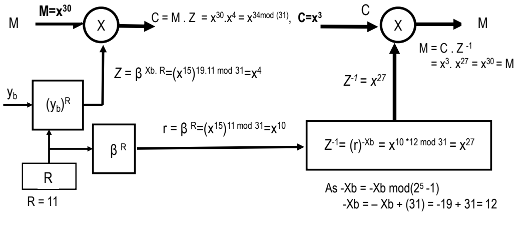
User A sends M to B

Xa =13
$y_a = \beta^{Xa} = x^4 + x^3 + x$

$\beta = x^{15}$ primitive element in $GF(2^5)$
$y_a = \beta^{Xa} = x^9 = 11010$
$y_b = \beta^{Xb} = x^6 = 01010$

User B receives

Xb = 19
$y_b = \beta^{Xb} = x^3 + x$



P3: Compute the multiplicative inverse of $x^2 + 1$ modulo $P(x) = x^7 + x^6 + 1$. **(6P)**

Verify your result

Solution

P1(x)	P2(x)	B1(x)	B2(x)	Q(x)	R(x)
$x^7 + x^6 + 1$	$x^2 + 1$	0	1	$x^5+x^4+x^3+x^2+x+1$	x
$x^2 + 1$	x	1	$x^5+x^4+x^3+x^2+x+1$	x	1
x	1	$x^5+x^4+x^3+x^2+x+1$	$x^6+x^5+x^4+x^3+x^2+x+1$	x	0

Check: $(x^2 + 1)(x^6+x^5+x^4+x^3+x^2+x+1)$

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

$= x^6 + x + 1 + x^6 + 1 + x + 1$

$= 1$

$x^7 = x^6 + 1$
$x^8 = x^7 + x = x^6 + x + 1$

P4: A block cipher having a key length of 194 bits is encrypting a clear text. Where, the clear text block size is 256 bits and the unicity distance of the cipher $n_u = 258$ bits. **(9 P)**

1. Compute the entropy of the clear text.

2. Compute the new unicity distance of the cipher if 64 random bits are appended to each clear text block. And the clear text is compressed to 50% of its original length.

3. Is the cipher theoretically breakable after this modification if the attacker can only observe 600 cipher text bits? Why?

Solution: K= 194 bits, n_u =258 bits, N = 256 bits

1. **Entropy of a clear text**

Unicity distance $n_u = K/r$ → **the redundancy is $r = K / n_u$** = 194/ 258 = **0,75**

As $r = [N - H(x)] / N \Rightarrow H(X)=N - N.r \Rightarrow H(x)=N(1-r)$

$H(x)=N(r-1)=256(1-0.75) = 64$ bits

← 256 bits block →	
192 bits compressed clear text H(x)=96 bits	64 bit random padding

2. New Unicity distance after compression

50% clear text compression results with a clear text entropy of 64 in each 128 bits block. Using the same cipher block size results with 192 bits compressed clear text data in each block + 64 bits random padding

After 50% compression each 128 bits clear text include 64 entropy bits, therefore The clear text entropy in the 192 bits is 192 x 64/128 = 96 bits. Therefore the new redundancy is: **r'=** 256-(96+64)/256 = **0,375.**

Therefore the **new unicity distance** is $n_u' = K/r'$ = 194/0,375 = **517,33 bits**.

3. After modifications, the observer can theoretically gain the secret key as the number of the observed cryptogram bits (600 bits) is greater than the new Unicity distance of the ciphering process (517 bits).

(35 P)

P5: El-Gamal crypto system is set up . A prime number P = 6 x 13 + 1 = 79 is used to generate GF(P), where q=13 is a prime.

1. **Prove that P is a prime according to Pocklington's theorem.**
2. **Find computationally the multiplicative orders of the elements 2 and 3 in GF(79). Compute the probability, that a randomly chosen element is a primitive one.**
3. **ElGamal signature scheme according to Fig .1 is used to sign M=6 in GF(79). The element $\alpha = 3$ is selected as a public group generator. Compute the signature S for M according to Fig.1. Assume $X_a = 13$ and select your own adequate K.**
4. **Encrypt the message M using a simple secret-key multiplication cipher $C(M) = K_s . M$ mod 79. Select $K_s = 32$. Compute the number of possible keys for this cipher.**
5. **Decrypt C(M)**
6. **Under which conditions is the cipher C(M) impossible to break ? Why?**

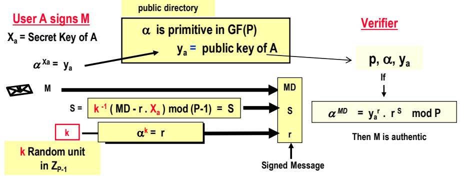


Fig. 1

Page 13

13

Solution:

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

P = R . F + 1 =6. 13 +1 = 79 , F =13 and R = 6. Is 79 a prime?

Proof: 1. gcd ($a^{(P-1)/pj}$ –1 , P) = gcd ($6^{138/23}$ –1 , 79) = gcd (63 , 139) = 1 is true

2. a^{P-1} = 1 (mod P) ⇔ 6^{78} = 1 (mod 79) is true

3. F > √79 = 8,xx that is 23 > 8,xx is true

As all conditions 1, 2 and 3 are all true ⇒ 79 is a prime number.

2. Find computationally the multiplicative orders of the elements 2 and 3 in GF(79). Compute the probability, that a randomly chosen element is a primitive one.

- Possible multiplicative orders are the divisors of of φ (79) = 78 that is => 1, **2,3,6,13,26,39**, 78
- Checking if the element 2 is a primitive one: $2^1 \neq 1$, $2^2 \neq 1$,$2^3 \neq 1$, $2^6 \neq 1$, 2^{13} =55≠ 1, 2^{26} =26 ≠ 1, 2^{39} =1,⇒ Ord (2) = 39 ⇒ 2 is not a primitive element.
- Checking if the element 3 is a primitive one: $3^1 \neq 1$, $3^2 \neq 1$,$3^3 \neq 1$, 3^6 =18≠ 1, 3^{13} =24≠ 1, 3^{26} =23 ≠ 1, 3^{39} =78 ≠ 1,⇒ Ord (3) = 78 ⇒ 3 is a primitive element

the probability that a randomly selected element is primitive.

\# of all non-zero elements : 79 – 1 = 78
\# of primitive elements: φ (78) = φ (2.3.13) = (2-1)(3-1)(13-1) = 24

P(element=primitive) = (24 / 78) . 100 = 30,77%

Page 14

14

3. ElGamal signature scheme according to Fig .1 is used to sign the message M=6 using GF(79). The element α = 3 is selected as a public group generator. Compute the multiplicative order of α and the Signature PS for M according to Fig.1. Assume X_a = 13 and select your own adequate K.

User A signs M=6

$\alpha^{Xa} = y_a = 3^{13}$ *mod 79 = 24*

Select k=5 => r = $\alpha^k = 3^5$ *mod 79 = 6*

Calculate k^{-1} *in* $Z_{P-1} = 5^{-1}$ *mod* (P-1)

k^{-1} *= -31 mod 78 =-31+78= 47*

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE = B2		GCD
78	5	1	0	0	1	15	3			
5	3	0	1	1	-15	1	2			
3	2	1	-1	-15	16	1	1			
2	1	-15	2	16	-31	2	0	INVERSE=	-31	GCD=

Signature S = k^{-1} (M - r . X_a) mod (P-1) = 47 (6 - 6.13) mod 78 = 47(6 - 0) mod 78 = 48

4. Encrypt the message M using a simple secret-key multiplication cipher C(M) = Ks . M mod 79. Select Ks = 32. Compute the number of possible keys for this cipher.

C(M) = K_S . M mod 79 = 32 x 6 mod 79 = 34 # possible keys for K_S = φ(79) = 78.

It is the number of invertible integers modulo 79,

5. Decrypt C(M)

Calculate the inverse key to retrieve M:

K_s=32, K_S^{-1} mod 79 = -37 mod 79 = -37 +79 = 42

=> M = K_S^{-1} . C(M) mod 79 = 42 x 34 mod 79 = 6

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE = B2		GCD
79	32	1	0	0	1	2	15			
32	15	0	1	1	-2	2	2			
15	2	1	-2	-2	5	7	1			
2	1	-2	15	5	-37	2	0	INVERSE=	-37	GCD=

6. Under which conditions is the cipher C(M) impossible to break ? Why?

As the modulus used in C(M) is a prime number, ciphering operates in a multiplicative group in GF(79).
The cipher is impossible to break if the key is not repeatedly used Key-length= clear text length. The cipher is then equivalent to a general Vernam Cipher. In that case Key Entropy = Clear text Entropy (Shannon perfect secrecy condition holds) Page 15

15

P6: **(15 P)**

A Massey-Omura lock for Shamir's 3-Pass Protocol is set up over GF(2^6) using the irreducible polynomial p(x) = $x^6 + x^4 + x^2 + x + 1$ as a field modulus.

1. **Compute the multiplicative order of x**
2. **The secret key for users A and B are 16 and 23 respectively. A message M = x^8 is sent from A to B. Compute all the exchanged 3-pass messages as powers of x with the smallest possible power of x.**
3. **Compute the number of possible distinct secret keys for each user**
4. **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 16

16

Solution:

1. **Write p(x) in binary form and find out the multiplicative order of x**

P(x) = $x^6 + x^4 + x^2 + x + 1 = 0$ => $x^6 = x^4 + x^2 + x + 1$

Possible multiplicative orders are the divisors of $2^6 - 1$ = **63 = 7 x 3^2**
Divisors of 63 are: 1, 3, 7, 9, 21, 63
Finding the order of x:
$x^1 \neq 1$, $x^3 \neq 1$, $x^7 = x^4 + x \neq 1$, $x^9 \neq 1$, $X^{21} = 1$
=> multiplicative order of x is 21

$x^1 = x$
$x^2 = x^2$
$x^3 = x^3$
$x^4 = x^4$
$x^5 = x^5$
$x^6 = x^4 + x^2 + x + 1$
$x^7 = x^5 + x^3 + x^2 + x$
$x^8 = x^6 + x^4 + x^3 + x^2$
$= x^4 + x^2 + x + 1 + x^4 + x^3 + x^2$
$= x^3 + x + 1$
$x^9 = x^4 + x^2 + x$
$x^{10} = x^5 + x^3 + x^2$
$X^{20} = (x^{10})^2 = x^{10} + x^6 + x^4$
$= x^5 + x^3 + x^2 + x^4 + x^2 + x + 1 + x^4$
$= x^5 + x^3 + x + 1$
$X^{21} = X^{20} x = x^6 + x^4 + x^2 + x$
$= x^4 + x^2 + x + 1 + x^4 + x^2 + x$
$= 1$

2. **E_a =16 and E_b =23 and their inverses D_a and D_b**

D_a

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE = B2		GCD	
63	16	1	0	0	1	3	15				
16	15	0	1	1	-3	1	1				
15	1	1	-1	-3	4	15	0	INVERSE=	4	GCD=	1

D_b

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE = B2		GCD
63	23	1	0	0	1	2	17			
23	17	0	1	1	-2	1	6			
17	6	1	-1	-2	3	2	5			
6	5	-2	3	3	-8	1	1			
5	1	3	-5	-8	11	5	0	INVERSE=	11	GCD=

Page 17

17

Solution :

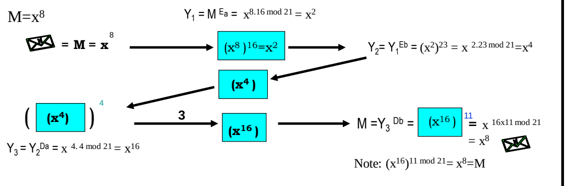
2.

User A **User B**

Arithmetic in GF(2^6)

E_a = 16
$D_a = E_a^{-1} = 16^{-1}$ mod 63 =4

E_b = 23
$D_b = E_b^{-1} = 23^{-1}$ mod 63 =11



3. Maximum # possible keys for each user = φ(2^6 -1) = φ(63) = φ(3^2*7) = 63* (1-1/3)*(1-1/7) = 36

4. In the most secure cases, and if a cleartext-cipher text pair is known, A maximum of 63 search cycles are required to find out E_a or E_b if M happens to be a primitive element. Only φ(2^6 -1) = φ(63) = 36 such Ms do exist.
In worst case, M may not be primitive and has an order of 3 (as possible orders are 3, 9, 21 or 63. in GF(2^6)).
This is the reason why when setting up GF(2^m), 2^m-1 should be selected as a prime number for highest security. In that case all messages, except the trivial message M=1 have the maximum order which is 2^m-1 and require that much cycles for revealing secret keys by a simple search..

Page 18

18