Examination sheets for:
Cryptology System Design Fundamentals

Grundlagen des kryptographischen Systementwurfs

Module ID: ET-IDA-28

Design problems section (open book exam)

Duration: 120 Minutes   13.02.2008

Name: ……………………………………………..

Matr. Nr.: ………………………………………..

Sample Solution

06-04.2021, v11

Contribution of : Martina Georgieva
Ivanov Stoyan

1

P1: **A RSA cryptosystem with two users A and B having the secret prime number pairs for A: 19 and 7 and for B: 17 and 5 is used** **(10 P)**

1. **Find out the adequate open key of user A from the following list of integers: [12, 21, 35]. Compute the corresponding secret key for user A.**
2. **Find out the adequate open key of user B from the following list of integers: [16,39,22]. Compute the corresponding secret key for user B..**
3. **User A encrypts the message M=3, and send the resulting cryptogram Y_B to B. The signature S_A of A for the message M is also sent to B. Compute Y_B and S_A.**
4. **Decipher the cryptogram Y_B on user B's site and verify the Signature S_A.**
5. **B signs the received message M and sends his signature S_B back to A. Compute the signature S_B.**
6. **How many open keys are possible for each user?**

2

Solution:

1. **Find out the adequate open key of user A from the following list of integers: [12, 21, 35]. Compute the corresponding secret key for user A.**

N_A = 19 x 7 = 133 , $\varphi(N_A)$ = (19-1)(7-1) = 108
gcd [E_A, $\varphi(N_A)$] = 1 => select 35 as gcd (35,108) = 1
E_A = 35
D_A = -37 mod 108 = 71 (see computation below)

$D_A = 35^{-1}$ mod 108 = - 37 =108-37= 71

m	u	b1	b2	q	r
108	35	0	1	3	3
35	3	1	-3	11	2
3	2	-3	34	1	1
2	1	34	-37	2	0

2. **Find out the adequate open key of user B from the following list of integers: [16,39,22]. Compute the corresponding secret key for user B.**

N_B = 17 x 5 = 85 , $\varphi(N_B)$ = (17-1)(5-1) = 64
gcd (E_B, $\varphi(N_B)$)] =1 => select 39 as gcd (39,64) = 1
E_B = 39
D_B = 23 mod 64 = 23 (see computation below)

$D_B = 39^{-1}$ mod 64 = 23

m	u	b1	b2	q	r
64	39	0	1	1	25
39	25	1	-1	1	14
25	14	-1	2	1	11
14	11	2	-3	1	3
11	3	-3	5	3	2
3	2	5	-18	1	1
2	1	-18	23	2	0

3

3. **User A encrypts the message M=3, and send the resulting cryptogram Y_B to B. The signature S_A of A for the message M is also sent to B. Compute Y_B and S_A.**

$Y_B = (M)^{E_B} \bmod N_B$ $S_A = (M)^{D_A} \bmod N_A$

$Y_B = (3)^{39} \bmod 85 = 62$ $S_A = (3)^{71} \bmod 133 = 89$

4. **Decipher the cryptogram Y_B on user B's site and verify the Signature S_A.**

Decryption:

$M = (Y_B)^{D_B} \bmod N_B$

$M = (62)^{23} \bmod 85 = (3^{39})^{23} \bmod 85$

$M = 3^{897 \bmod 64} \bmod 85 = 3^1$

Verification:

check if : $(S_A)^{E_A} \bmod N_A = M$

$(3^{71})^{35} \bmod 133 = 3$

$3^{2485 \bmod 108} \bmod 133 = 3$

$3^1 \bmod 133 = 3$

$3 = 3 = M$ => signature is authentic!

5. **B signs the received message M and sends his signature S_B back to A. Compute the signature S_B.**

$S_B = (M)^{D_B} \bmod N_B$

$S_B = (3)^{23} \bmod 85 = 62$

6. **How many open keys are possible for each user?**

# of keys for user A = φ [φ (N_A)] = φ (108) = φ (2.2.3.3.3)= 108 (1 -1/2) (1 – 1/3) = **36 keys**
# of keys for user B = φ [φ (N_B)] = φ (64) = φ (2^6)= 64 (1 -1/2) = **32 keys**

4

P2: **A block cipher having a key size of 56 bits is encrypting a clear text with the entropy of 90 bits. The clear text redundancy is r=0.1.** **(8 P)**

1. **Compute the cipher's unicity distance n_u and its block length N.**
2. **The unicity distance was doubled by data compression. Compute the new resulting data block length.**
3. **After compression as in (2), the „unicity distance" was enhanced by appending 10 random bits to the clear text block. Compute the new resulting unicity distance.**
4. **After all the above cipher changes an observer was able to watch 1000 cipher text bits. Would the observer with unlimited resources theoretically be able to break the cipher in that case ? Give a reasoning for your answer.**

5

Solution:

K= 56 Bits, H(x)=90 Bits, r = 0.1

1. Unicity distance n_u = K/r = 56/0.1 = 560 Bits

As r = [N – H(x)] / N
=> N . r = N – H(x) => Block size **N = H(x) / (1-r)** => N = 90/0.9 = 100 Bits

2. New unicity distance n'_u = 2 x 560 = 1120 Bits

n'_u = K/r' => r' = K/n'_u => the new resundancy r'= 56/1120 = 0.05

The new block size N' = H(x) / (1-r') = 90 / (1 – 0.05) = 94.74 ≈ 95 Bits

3. n''_u = (L + N) / N · n'_u = (10 + 95)/95 x 1120
n''_u ≈ 1238 Bits

4. The observer can not theoretically break the cipher as the number of the observed cryptogram bits (1000 bits) are less than the unicity disctance (1238 bits) of the cipher.

6

P3: A Diffie-Hellman (DH) public key exchange system uses GF(2^6) deploying the **irreducible** Polynomial $P(x) = x^6 + x^3 + 1$ as field modulus. **(15 P)**

1. Compute the exponents of the element $\delta = x = 000010$ as $x^i \bmod P(x)$ for i= 1 to 10 and find the multiplicative order of the element x.
2. Which multiplicative orders are possible in GF(2^6)?
3. $\beta = (1+x^3)$ is an element in GF(2^6). Compute the multiplicative order of β. (Hint make use of the fact that $1+x^3 = x^6$).
4. Use the element $\alpha=(1+x)$ as a primitive element and compute the DH public keys and the shared key Z_{AB} for users A and B having the secret keys $X_a=32$ und $X_b=57$.
5. Compute the multiplicative order of $(1+x)^{45}$. Compute also all elements having the same order.
6. What is the probability of picking up a primitive element in GF(2^6) if such element is randomly selected?.

Hints

$\alpha=(1+x)$, $\alpha^3= 1+x+x^2+x^3$, $\alpha^7= x^2+x^5$, $\alpha^9= x+x^2+x^5$, $\alpha^{20}= 1+x+x^2$, $\alpha^{21}= 1+x^3$

7

Solution:

1. Compute the exponents of the element $\delta=x = 000010$ as $x^i \bmod P(x)$ for i= 1 to 10 and find the multiplicative order of the element x.

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

$x^1 = x$
$x^2 = x^2$
$x^3 = x^3$
$x^4 = x^4$
$x^5 = x^5$
$x^6 = x^3 + 1$
$x^7 = x^4 + x$
$x^8 = x^5 + x^2$
$x^9 = x^6 + x^3 = x^3 + 1 + x^3 = 1$ => multiplicative order of x is 9
$x^{10} = x$

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

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

3. $\beta= (1+x^3)$ is an element in GF(2^6). Compute the multiplicative order of β. (Hint make use of the fact that $1+x^3 = x^6$).

$\beta= (1 + x^3)$ as $x^3 + 1 = x^6$ => $\beta= x^6$,
Note: ord (x) = 9 (see solution 1)
ord (β) = ord (x^6) = ord x / gcd (ord x , 6) = 9 / gcd (9,6) = 9 / 3 = 3 => ord (β) = 3

8

4. Use the element $\alpha=(1+x)$ as a primitive element and compute the DH public keys and the shared key Z_{AB} for users A and B having the secret keys $X_a=32$ und $X_b=57$.

Hints: $\alpha=(1+x)$, $\alpha^3= 1+x+x^2+x^3$, $\alpha^7= x^2+x^5$, $\alpha^9= x+x^2+x^5$, $\alpha^{20}= 1+x+x^2$, $\alpha^{21}= 1+x^3$

User A:
$X_a= 32$,
$Y_a = \alpha^{32} = x^4$

Public directory GF(2^6)
$\alpha=(1+x)$, $P(x) = x^6 + x^3 + 1$
$Y_a = \alpha^{32}$
$Y_b = \alpha^{57}$

User B:
$X_b= 57$,
$Y_b = \alpha^{57}$

$x^6 = \cancel{x^3} + \cancel{1}$

Common secret key for users A and B

$Z_{ab} = (\alpha^{32})^{57} = (\alpha^{57})^{32} = \alpha^{1824 \bmod 63} = \alpha^{60} = (\alpha^{20})^2 \alpha^{20} = (1+x^2+x^4)(1+x+x^2) = \cancel{1}+\cancel{x^2}+\cancel{x^4} + x + \cancel{x^3}+x^5 + \cancel{x^2}+\cancel{x^4}+\cancel{x^6} = x + x^5 = 100010$

$\boxed{Z_{ab} = x + x^5 = 100010}$ **Remark:** ord(α) = 63

5. Compute the multiplicative order of $(1+x)^{45}$. Compute also all elements having the same order.

$$ord(\alpha^i) = \frac{ord(\alpha)}{\gcd[ord(\alpha), i]}$$

$$ord(\alpha^{45}) = \frac{63}{\gcd[63,45]} = \frac{63}{9} = 7$$

Let $\alpha^{45} = \sigma$ $\quad ord(\sigma^i) = \frac{ord(\sigma)}{\gcd[ord(\sigma), i]}$

if $\gcd[ord(\sigma), i] = 1$ then: $ord(\sigma^i) = ord(\sigma)$
that is i should be selected such that, $\gcd(7, i) = 1$

The other elemets having the same order as that of σ are then:
$\sigma^2, \sigma^3, \sigma^4, \sigma^5, \sigma^6$
$\alpha^{90 \bmod 63}, \alpha^{135 \bmod 63}, \alpha^{180 \bmod 63}, \alpha^{225 \bmod 63}, \alpha^{270 \bmod 63}$
$\alpha^{27}, \alpha^{9}, \alpha^{54}, \alpha^{36}, \alpha^{18}$ all have the order 7
$\alpha^7 \alpha^{20}$ $\quad \alpha^9 = x+x^2+x^5$

9

P4: **(6 P)**

Compute the multiplicative inverse of $x^5 + x^4$ modulo $P(x) = x^9 + x^8 + 1$. P(x) is an irreducible polynomial. Compute the possible multiplicative orders for elements in GF(2^9).

1. **Extended gcd Algorithm:**

$\boxed{B2 = B1 - q\,B2}$

$P_1(x)$	$P_2(x)$	B1(x)	B2(x)	Q(x)	R(x)
$x^9 + x^8 + 1$	$x^5 + x^4$	0	1	x^4	1
$x^5 + x^4$	1	1	$0 - (x^4) \cdot 1 = x^4$	$x^5 + x^4$	0

$P(x) = x^9 + x^8 + 1 \Rightarrow x^9 = x^8 + 1$

=> $(x^4) \equiv (x^5 + x^4)^{-1}$ modulo $(x^9 + x^8 + 1)$

$x^9 = x^8 + 1$
Check: $(x^4) \cdot (x^5 + x^4) = x^8 + x^9 = x^8 + x^8 + 1 = 1$

2. Possible orders are the divisors of $2^9 - 1 = 511 = 7 \cdot 73$

=> Possible orders are : 1, 7, 73, 511

Name:_________________ Matr.Nr.:___________________ Page 3/5

10

(8 P)

P5: El-Gamal crypto system is set up using the prime number N=2 x 41 + 1 = 83 generated by applying Pocklington's Theorem, where q=41 is prime.

1. Prove that N is prime according to Pocklington's Theorem.
2. Seek a primitive element for the public directory. Furthermore compute the probability that a randomly selected element is primitive.
3. User A having the secret key $X_a= 7$ receives C_a as encrypted message M=23 using the random number K=4. Compute Y_a and C_a .
4. Decrypt the cryptogram C_a on the receiver side showing all necessary computation therefore.

11

Solution:

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

N = R . F + 1 = 2 . 41 + 1 = 83, F = 41 and R = 2. Is 83 a prime?

Proof: 1. $\gcd(a^{(N-1)/pj} - 1, N) = \gcd(2^{82/41} - 1, 83) = \gcd(3, 83) = 1$ is true

2. $a^{N-1} = 1 \pmod N \Leftrightarrow 2^{82} = 1 \pmod{83}$ is true

3. $F > \sqrt{83} \Rightarrow 41 > 9{,}1$ is true

As all conditions 1, 2 and 3 are all true $\Rightarrow$ 83 is prime

2. Seek a primitive element for the public directory. Furthermore, compute the probability that a randomly selected element is a primitive one.

Possible multiplicative orders are the divisors of of $\varphi(83) = 82 = 2 . 41$
that is => 1, 2, 41, 82
Checking if the element 2 is a primitive one:
$2^1 \neq 1$, $2^2 \neq 1$, $2^{41} = 82 \neq 1 \Rightarrow$ Ord (2) = 82 $\Rightarrow$ 2 is primitive element

# of all non-zero elements : 83 – 1 = 82
# of primitive elements: $\varphi(82) = \varphi(2 . 41) = 40$

Pr(element=primitive) = (40 / 82) . 100 = 48,78%

12

3. User A having the secret key $X_a = 7$ receives C_a as the encrypted message M = 23 using the random number K = 4. Compute Y_a and C_a.

Encryption:

User A.
$X_a = 7$
$Y_a = \alpha^{X_a} = 2^7 = 45$

Public directory
$\alpha = 2$, GF(83)
$Y_a = 2^7 = 45$

User B.
M = 23
K = 4

C_a: [C=64, r =16]

$C_a \begin{cases} r = \alpha^K = 2^4 = \mathbf{16} \\ C = M \cdot Y_a^K = 23 \cdot (2^7)^4 = 23 \; 2^{28} = \mathbf{64} \end{cases}$

Decryption:

mod 82

$Z^{-1} = (\alpha^K)^{-X_a} = r^{-X_a} = (2^4)^{-7} = 2^{-28+82} = 2^{54} = 25$
$M = C \cdot Z^{-1} = 64 \cdot 25 \mod 83 = 23$

Or $M = C \cdot r^{-X_a} = 23 \cdot 2^{28} \cdot 2^{54} = 23 \cdot 2^{82 \bmod 82} = \mathbf{23}$ (mod 83)

13

P6: Omura proof-of-identity protocol uses GF(53) arithmetic is set up: **(12 P)**

1. How many primitive elements do exist in GF(53)?
2. Compute the probability that a randomly selected element is primitive in GF(53).
3. Compute the order of the element α =3
4. Use α as an open reference element for the above Omura proof-of-identity protocol system. Generate a "Challenge" by using the random integer K=15 to prove the identity of user A whose secret key is X_A=7. Compute the response of user A and show all necessary computations to verify his/her identity.

14

Solution:

1. How many primitive elements do exist in GF(53)?

The order of the primitive element = 53-1 =52
Number of primitive elements is $\varphi(52)$:
$\varphi(52) = \varphi(2^2 \cdot 13) = 52(1 - 1/2)(1 - 1/13) = \frac{\cancel{52}\,4 \cdot 1 \cdot \cancel{12}\,6}{\cancel{2} \cdot \cancel{13}} = \mathbf{24}$

2. Compute the probability that a randomly selected element is primitive in GF(53).

\# of non-zero elements : 53 – 1 = 52
\# of primitive elements: $\varphi(52) = 24$

Pr(element=primitive) = (24 / 52) . 100 = 46,15%

3. Compute the order of the element α =3

Possible orders are the divisors of of 52, that is : 1, 2, 4, 13, 26, 52

Checking the order of the element α =3:
$3^1 = 3 \neq 1$; $3^2 = 9 \neq 1$; $3^4 = 28 \neq 1$;

$3^{13} = 3^4 \cdot 3^4 \cdot 3^4 \cdot 3 = 30 \neq 1$; $3^{26} = 3^{13} \cdot 3^{13} = 52 \neq 1$ $\Rightarrow$ **Ord (3) = 52**

15

4. Use α as an open reference element for the above Omura proof-of-identity protocol system. Generate a "Challenge" by using the random integer K=15 to prove the identity of user A who's secret key is X_A=7. Compute the response of user A and show all necessary computations to verify his/her identity

Prover
$X_A = 7$
$Y_A = \alpha^{X_A} = 3^7$

PUBLIC :
GF(53)
$\alpha = 3$
$Y_A = 3^7 = 14$

Verifier
K = 15
$R = \alpha^K = 3^{15} = 5$

R = 5

$Z = R^{X_A} = 5^7 = (3^{15})^7$
$= 3^{105 \bmod 52} = 3^1$

$R^{X_A} = \mathbf{3}$

$R^{X_A} = Y_A^K$?

$3 = (3^7)^{15} = 3^{105 \bmod 52} \mod 53 = 3$
$3^1 = 3^1 \Rightarrow$ is true, A's identity is authentic

16

P7: Sketch Massey-Omura lock for Shamir's 3-Pass Protocol over GF(2^6) using the primitive polynomial modulus $p(x) = 1 + x + x^6$. **(12 P)**

1. Compute the number of all possible secret keys for each user.
2. The secret key for users A and B are 31 and 19 respectively. Compute all the exchanged messages and show all necessary computations for a message M = x = 000010.

Solution:

GF (2^6) $p(x) = 1 + x + x^6$

1. Compute the number of all possible secret keys for each user.

Condition for a valid key E_A is: gcd (E_A , 2^6 - 1) = 1 or gcd (E_A , 63) = 1

The number of possible keys is then φ (63)

$\Rightarrow$ $\mathbf{\#E_A = \varphi(63)} = \varphi(3^2 \cdot 7) = 63(1 - 1/3)(1 - 1/7) = 63\,(2/3)\,(6/7) =$ **36** secret keys

17

2. The secret key for users A and B are 31 and 19 respectively. Compute all the exchanged messages and show all necessary computations for a message M = x = 000010.

User A

Modulus in the exponent $= 2^6 - 1 = 63$

User B

$E_a = 31$
$D_a = 31^{-1} = -2 \mod 63 = -2+63 = 61$

$E_b = 19$
$D_b = 10$

M = x = 000010 $\xrightarrow{Y_1 = M^{E_a} = x^{31}}$ $Y_2 = Y_1^{E_b} = (x^{31})^{19} = x^{589 \bmod 63} = x^{22}$

$Y_2 = x^{22}$

$Y_2 = x^{22}$
$Y_3 = Y_2^{D_a} = (x^{22})^{61} = x^{61.22 \bmod 63} = x^{19}$ $\xrightarrow{Y_3 = x^{19}}$ $\mathbf{Y_3^{D_b}} = (x^{19})^{10} = x^{190 \bmod 63} = \mathbf{x^1 = M}$

$D_a = E_a^{-1} \mod 63 = -2 = \underline{\mathbf{61}}$

n_1	n_2	a_1	a_2	b_1	b_2	q	r
63	31	1	0	0	1	2	1
31	1	0	1	1	-2	31	0

$D_b = E_b^{-1} \mod 63 = \underline{\mathbf{10}}$

n_1	n_2	a_1	a_2	b_1	b_2	q	r
63	19	1	0	0	1	3	6
19	6	0	1	1	-3	3	1
6	1	1	-3	-3	10	6	0

18