Introduction to Cryptology

Midterm Examination
Open book examination

V9-31.05.2023

Sample Solution

Date : 26-04-2023
Duration : 120 Minuets

First name ....
Family name ....
Regl-Nr. ....
Dept: ....

Marks:

Total	

1

2

Q1: For the following pairs (m = 125 , u = 65) of integers find gcd (m, u) and the integers a, b such that gcd (m , u) = a . m + b . u (4 P)

Solution:

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE = B2		GCD	
125	65	1	0	0	1	1	60				
65	60	0	1	1	-1	1	5				
60	5	1	-1	-1	2	12	0	NVERSE=		GCD=	5

$\Rightarrow$ gcd (125,65) = 5
$\Rightarrow$ b = 2
$\Rightarrow$ a = -1

Q2: Compute $\gcd[(4^{68}-1,\ 16^{152}-1)]$ (2 P)

$= [\ 4^{68}-1, 4^{2\cdot 152}-1\ ]$
$= [\ 4^{\gcd(68,2\cdot 152)}-1\ ]$
$= [\ 4^{\gcd(304,68)}-1\ ]$
$= [\ 4^{4}-1\ ]$
$= [\ 256-1\ ]$
$= 255$

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE = B2		GCD	
304	68	1	0	0	1	4	32				
68	32	0	1	1	-4	2	4				
32	4	1	-2	-4	9	8	0	NVERSE=		GCD=	4

3

Q3: Compute the multiplicative order of 7^7 in GF(127) knowing that 7 is a primitive element in GF(127). (4 P)
Since ord(7) = 127-1 = 126

$$ord(\alpha^i) = \frac{ord(\alpha)}{\gcd[ord(\alpha), i]} \Rightarrow ord(7^7) = \frac{126}{\gcd[126,7]} = \frac{126}{7} = 18$$

Q4: How many elements are there in the group of units Z^*_m for m = 5 • 23 =115. (9 P)

- Compute the highest possible multiplicative order for a unit in Z^*_m?
Highest possible order is: $\lambda(5\ .\ 23)$ = lcm [$\lambda(5)$, $\lambda(23)$]
= lcm [$\varphi(5)$, $\varphi(23)$] = lcm [4, 22]
= 4 . 22 / gcd(4,22) = 88/2 = 44

- How many elements are there in Z^*_m
# of elements in the group is $\varphi(5\ .\ 23)$ = (5-1) (23-1) = 88

- Compute the multiplicative order of the element 2:
Possible orders are the divisors of $\lambda(115)$=44=2 x 2 x 11 which are 1, 2, 4, 11, 22, 44
$2^1 \neq 1$, $2^2 = 4 \neq 1$, $2^4 = 16 \neq 1$, $2^{11} = 93 \neq 1$, $2^{22} = 24 \neq 1$ => order of 2 is 44

4

Q5: Reduce the following expressions to the smallest positive integers in the corresponding deployed algebra: (4 P)

1. R_{39} (41 ^{3} – (33) ^{2} · 38 ^{33}) =

   = R_{39} ($(2)^3$ – (-6) ^{2} · $(-1)^{33}$)
   = R_{39} (8 – (36 · -1))
   = R_{39} (8 + 36)
   = 44 mod 39 = 5

2. (2 + 5x ^{3}) (7 - 4x^3 - 5x^5) over GF(11) =

   = 14 – 8x^3 – 10x^5 + 35 x^3 - 20x^6 - 25x^8
   = 3 – 8x^3 – 10x^5 + 2 x^3 - 9x^6 - 3x^8
   = 8x^8 + 2x^6 + 1x^5 +5x^3 + 3

5

Q6: Are the following sentences true or false? Give the reason for your answer. (5 P)

1) **The order of the element x modulo any irreducible polynomial over GF(2^m) is $2^m - 1$.**

   False, This holds only for primitive irreducible polynomial

2) **A primitive group's element is an element having the maximum possible order.**

   True

6

Q7: In GF(59). (8 P)

1. Compute the possible multiplicative orders for the multiplicative group in the field.

Possible multiplicative orders are the divisors of $\varphi(59) = 58$.
These are: 1,2,29 and 58

2. Compute the number of primitive elements.

\# of primitive elements $\varphi(58) = \varphi(2.29) = 2\cdot29\,(1-1/2)(1-1/29) = 28$

3. Which minimum number of tests are required to find out whether a given element β is primitive?

$\beta^1 \neq 1$, $\beta^2 \neq 1$ and $\beta^{29} \neq 1$ (three tests are required)

4. Compute the multiplicative order of 3.

$3^1 \neq 1$, $3^2 = 9 \neq 1$, $3^{29} = 1$ => order of 3 is 29

5. Compute 3^{-170} by computing the smallest positive integer t, for which $3^{-170} = 3^t$ holds.

$3^{-170} = 3^t = 3^{-170 \bmod 29} = 3^{25}$
=> t = 25

Remark :
- As the order of a is 29, the smallest modulus in the exponent is 29
- the modulus 58 is usable however, would not deliver the smallest t

Q8: $GF(2^7)$ is generated by the irreducible polynomial P(x)= (11001011) (12 P)
The element ß = 0010001 = $x^4 + 1$ is selected from $GF(2^7)$.
[hint $(2^7 - 1) = 127$=prime]

1. Compute the multiplicative order of ß = $x^4 + 1$

Possible orders are divisors of 127: these are 1 and 127
since: $(x^4 + 1)^1 \neq 1$, then
=> the multipicative order of ß is 127

2. Compute $ß^2$ and give the corresponding binary vector of $ß^2$.

P(x)= $x^7 + x^6 + x^3 + x + 1 = 0$ => $x^7 = x^6 + x^3 + x + 1$
ß = $x^4 + 1$ => $ß^2 = x^8 + 1$

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

$ß^2 = x^8 + 1 = x^6 + x^4 + x^3 + x^2 + \cancel{1} + \cancel{1} = x^6 + x^4 + x^3 + x^2$
= 1011100

3. Compute the smallest positive integer t for which $ß^{-120} = ß^t$ holds.

$ß^{-120 \bmod 127} = ß^{-120+127} = ß^7 = ß^t$ => t = 7

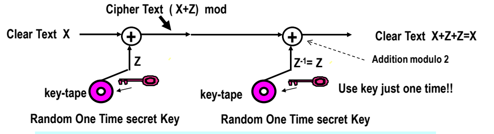
Remark : As the order of a is 127, the smallest modulus in the exponent is 127

4. Compute the binary vector corresponding to $(x^5 + x^2 + 1)^2$.
$(x^5 + x^2 + 1)^2 = (x^{10} + x^4 + 1)$

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

Substituting in $x^{10} + x^4 + 1 = x^5 + x^3 + 1 + x^4 + 1 = x^5 + x^4 + x^3$ = 0111000

Q9: Sketch the scheme of one unconditionally secure cipher and set the necessary operation conditions therefore. (4 P)



Unconditional Secrecy if : Key length = Clear text length (Shannon 1949)

Or H(z) > H(X)

Q 10: What is the difference between an irreducible and a primitive polynomial? (4 P)

irreducible polynomial: A polynomial of degree m is said to be irreducible if it cannot be factored into nontrivial polynomials over the same field. If the order of x modulo that polynomial is 2^m-1, then it is said to be primitive polynomial.
<u>In other words:</u>
The order of x for any irreducible polynomial is a divisor of 2^m-1 if the order of x is maximum (that is 2^m-1) then the polynomial is said to be a primitive polynomial).

Q11: 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: $(x^2 + 1)(x^6+x^5+x^4+x^3+x^2+x+1)$
$= x^8+x^7+x^6+x^5+x^4+x^3+x^2+ x^6+x^5+x^4+x^3+x^2+x+1$
$= x^6 + x + 1 + x^6 + 1 + x + 1$
$= 1$

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

Q12: (9 P)

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.

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 the 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 => H(X)=N –N.r => H(x)=N(1-r)

Clear text entropy H(x) = N(1-r) = 256(1-0.75) = 64 bits

2. New Unicity distance after compression

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

50% clear text block compression results with unchanged clear text entropy of 64 bits in each 128 bits compressed block.
Using the same cipher block size results with 192 compressed clear text bits in each 256 bits block + 64 bits random padding. The clear text entropy in the 192 bits is 192 x 64/128 = 96 bits. 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 reveal the secret key as the number of the observed cryptogram bits is 600 bits which is greater than the new Unicity distance of (517 bits).

Q13: (35 P)

A crypto-system requires to create a prime number. The number P =2 x (3x13) + 1 = 79 is proposed to be used to generate GF(P), where 13 and 3 are two primes.

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. 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 usable keys for this cipher.
4. Decrypt C(M)
5. Under which conditions is the cipher C(M) impossible to break ? Why?

Solution:

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

P = R . F + 1 = 2 (3x13) +1 = 79 , F = 3x13 and R = 2. Is 79 a prime?

Proof: 1. select a=6, a^{P-1} = 1 (mod P) ⇔ 6^{78} = 1 (mod 79) is true

2. gcd ($a^{(P-1)/pj}$ –1 , P) = gcd ($6^{78/3}$ –1 , 79) = gcd (6^{26} , 79) = 1 is true
gcd ($a^{(P-1)/pj}$ –1 , P) = gcd ($6^{78/13}$ –1 , 79) = gcd (6^{6} , 79) = 1 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 for sure 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%

3. 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.

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,

4. Decrypt C(M)

Calculate the inverse key to retrieve M:

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

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

5. 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 then equivalent to a general Vernam Cipher.
The cipher is impossible to break if the key is not repeatedly used: Key-length= clear text length.
It is unbreakable if Key Entropy ≥ Clear text Entropy (Shannon perfect secrecy condition holds)

Annex:

gcd (t^n-1, t^m-1) = $t^{\gcd(n, m)}$ - 1

Euler Function ϕ(m)

For m = $p_1^{e_1} \; p_2^{e_2} \; p_3^{e_3} \ldots\; p_t^{e_t}$ ⟶ $\phi(m) = m\left(1 - \frac{1}{P_1}\right)\left(1 - \frac{1}{P_2}\right) \ldots\ldots$

Carmicheal´s function λ(m) :

λ (2)= 1, λ(2^2) = 2, λ(2^e) = 2^{e-2} for e ≥ 3:

λ(p^e)= Φ(p^e) = (p - 1)p^{e-1} for p odd prim.

for m = p_1^{e1} p_2^{e2} p_3^{e3} ... p_n^{en}

λ(m) = lcm [λ(p_1^{e1}), λ(p_2^{e2}), ... λ(p_n^{en})]

$$\text{lcm}(a,b) = \frac{a \cdot b}{\gcd(a,b)}.$$

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