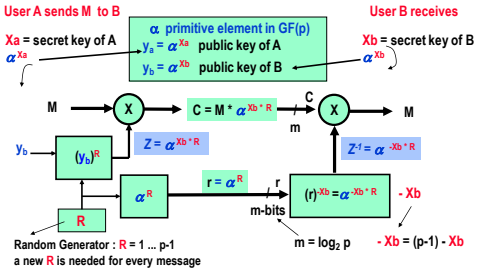
Introduction to Cryptology

Tutorial-09

ElGamal Public-Key Systems over GF(p) & GF(2^m)

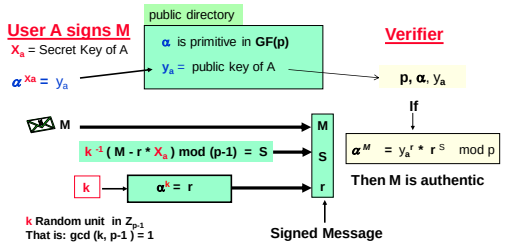
15.05.2023, v52

ElGamal Secrecy-System (1985)



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

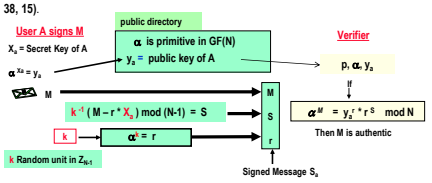
ElGamal Signature Scheme



ElGamal Secrecy-System Over GF (p)

Problem 9-1: El-Gamal crypto system is set up using the prime number **N = 2 * 19 * 11 + 1 = 419** generated by applying Pocklington's Theorem, where **19** and **11** are two primes.

1. Prove that N is a prime according to Pocklington's Theorem.
2. Compute the probability that a randomly selected element is primitive in **GF(419)**.
3. Find a primitive element in **GF(419)** and use it as a public element in El-Gamal public key system.
4. User A encrypts the message **M = 21** and send it to user B who has the secret key X_b **= 80** by using the random number **R = 13**. Compute B's public key Y_b and the encrypted message C_a and r.
5. Decrypt the cryptogram C_a on the receiver side B showing all therefore necessary computations.
6. Let user A having the secret key X_a **= 133** compute his Signature S_a according to El-Gamal signature scheme shown below for the same message **M = 21**. Select one adequate k from the following list **(k = 22, 38, 15)**.



Solution 9-1:

1. N = R * F + 1= 2 * 19 * 11 + 1 = 419, F = 19 * 11 and R = 2. p1 = 19, p2 = 11 Is 419 a prime?
   Proof: We select a = 2
   1. gcd ($a^{(N-1)/p1} - 1$, N) = gcd ($2^{22} - 1$, 419) = 1 is true
      gcd ($a^{(N-1)/p2} - 1$, N) = gcd ($2^{38} - 1$, 419) = 1 is true
   2. $a^{N-1} = 1 \pmod N \Leftrightarrow 2^{419} = 1 \pmod{419}$ is true
   3. F > √N
      11 * 19 > √419 = 20.46 ⇒ 209 > 20.46 is true
   As all conditions 1, 2 and 3 are true ⇒ 419 is prime
2. # of all non-zero elements : 419 – 1 = 418
   # of primitive elements: φ (418) = φ (2 * 11 * 19) = (2 – 1) * (11 – 1) * (19 – 1) = 180
   P(element=primitive) = (180 / 418) * 100 = 43.06%
3. Possible orders are the divisors of 419 – 1 = 418
   These are: 1, 2, 11, 19, 22, 38, 209 and 418

   Checking if the element 2 is primitive
   $2^1 \bmod 419 \neq 1$, $2^{22} \bmod 419 \neq 1$
   $2^2 \bmod 419 \neq 1$, $2^{38} \bmod 419 \neq 1$
   $2^{11} \bmod 419 \neq 1$, $2^{209} \bmod 419 \neq 1$ ⇒ Ord(2) = 418 ⇒ 2 is primitive element
   $2^{19} \bmod 419 \neq 1$

Solution 9-1 cont.:

4. Encryption:

User A: M = 21

Public directory: α = 2, GF(419); Y_b = 375

User B: X_b = 80; $Y_b = \alpha^{X_b} \bmod N = 2^{80} \bmod 419 = 375$

$r = \alpha^R = 2^{13} \bmod 419 = 231$

$C_a = M * Y_b^R = (21 * 375^{13}) \bmod 419 = 91$

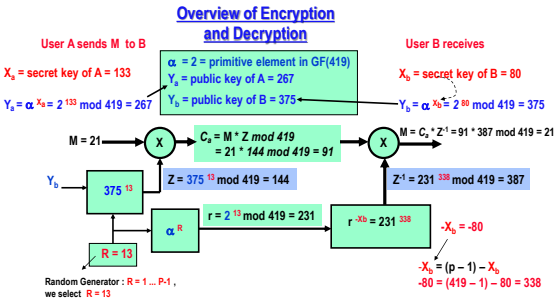
5. Decryption:

$Z^{-1} = r^{-X_b} = 231^{-80 \bmod 418} \bmod 419 = 231^{-80+418} \bmod 419 = 387$

$M = C_a * Z^{-1} = 91 * 387 \bmod 419 = 21$

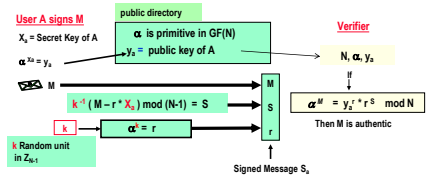
Solution 9-1 cont.:

Overview of Encryption and Decryption



Solution 9-1 cont.:

6.



k has to be invertible mod N-1, N-1 = 418

gcd [k, N-1] = 1 => select 15 as gcd (418,15) = 1

k = 15, $k^{-1} = 15^{-1} = -195 \bmod 418 = 223$ (see table below)

$r = \alpha^k = 2^{15} \bmod 419 = 86$

$S = k^{-1} (M - r * X_a) \bmod (N-1)$

$= 15^{-1}(21 - 86 * 133) \bmod 418$

$= 223 (21 - 11438) \bmod 418$

$= -2545991 \bmod 418$

S = 47

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE =		GC
418	15	1	0	0	1	27	13			
15	13	0	1	1	-27	1	2			
13	2	1	-1	-27	28	6	1			
2	1	-1	7	28	-195	2	0	INVERSE=	-195	GCD=

Problem 9-2: El-Gamal crypto system is set up using the prime number N = 29.

1. Find a primitive element in **GF(29)** and use it as a public element in El-Gamal public key system.
2. User A has the secret key $X_a = 7$ and User B has the secret key $X_b = 4$. Compute A's public key Y_a and B's public key Y_b.
3. User A encrypts the message **M = 17** and send it to user B. Compute the encrypted message C_a and r.
   a. Use the random number **R = 21**.
   b. Use the random number **R = 25**.
   c. Which random number is better? Why?
4. Decrypt the cryptogram C_a on the receiver side B showing all necessary computations therefore. Use the better random number R.

Solution 9-2:

1. Possible orders are the divisors of 29 – 1 = 28
   These are: 1, 2, 4, 7, 14 and 28

   Checking if the element 3 is primitive
   $3^1 \bmod 29 \neq 1$
   $3^2 \bmod 29 \neq 1$
   $3^4 \bmod 29 \neq 1$
   $3^7 \bmod 29 \neq 1$
   $3^{14} \bmod 29 \neq 1$ $\Rightarrow$ Ord(3) = 28 $\Rightarrow$ 3 is primitive element

Solution 9-2 cont.:

2. User A: $X_a = 7$
   $Y_a = \alpha^{X_a} \bmod N = 3^7 \bmod 29 = 12$

   User B: $X_b = 4$
   $Y_b = \alpha^{X_b} \bmod N = 3^4 \bmod 29 = 23$

3.a. User A: $X_b = 7$, M = 17, R = 21

Public directory: α = 2, GF(29); Y_a = 12; Y_b = 23

User B: $X_b = 4$

$r = \alpha^R = 3^{21} \bmod 29 = 17$

$C_a = M * Y_b^R = (17 * 23^{21}) \bmod 29 = 17$

3.b. User A: $X_b = 7$, M = 17, R = 25

Public directory: α = 2, GF(29); Y_a = 12; Y_b = 23

User B: $X_b = 4$

$r = \alpha^R = 3^{25} \bmod 29 = 14$

$C_a = M * Y_b^R = (17 * 23^{25}) \bmod 29 = 21$

Solution 9-2 cont.:

3.c. The random number R = 25 is better, because the random number R = 21 has the consequence that $C_a = M$. So there is no encryption, when using R = 21.

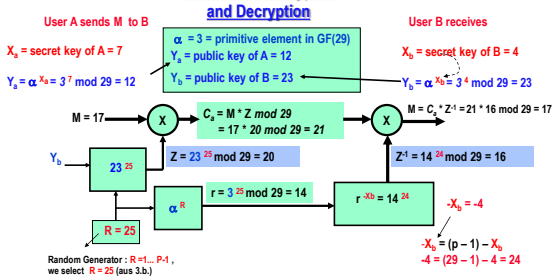
5. Decryption:

$Z^{-1} = r^{-X_b} = 14^{-4 \bmod 28} \bmod 29 = 14^{-4+28} \bmod 29 = 16$

$M = C_a * Z^{-1} = 21 * 16 \bmod 29 = 17$

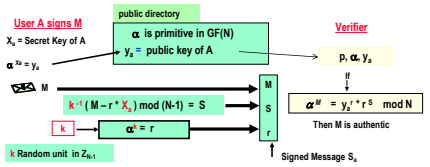
Solution 9-2 cont.:

Overview of Encryption and Decryption



Problem 9-3: El-Gamal crypto system is set up using the prime number **N = 2 * 131 + 1 = 263** generated by applying Pocklington's Theorem, where **131** is a prime.

1. Prove that N is a prime according to Pocklington's Theorem.
2. Compute the probability that a randomly selected element is primitive in **GF(263)**.
3. Find a primitive element in **GF(263)** and use it as a public element in El-Gamal public key system.
4. User A encrypts the message **M = 35** and send it to user B who has the secret key X_b **= 113** by using the random number **R = 22**. Compute B's public key Y_b and the encrypted message C_a and r.
5. Decrypt the cryptogram C_a on the receiver side B showing all necessary computations therefore.
6. Let user A having the secret key X_a **= 40** compute his Signature S_a according to El-Gamal signature scheme shown below for the same message **M = 35**. Choose **k = 121**.



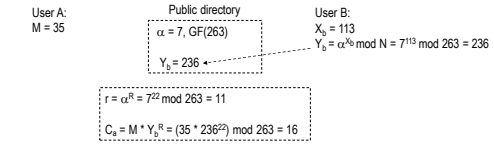
Solution 9-3:

1. N = R * F + 1= 2 * 131 + 1 = 263, F = p = 131 and R = 2. Is 263 a prime?
   Proof: We select a = 11
   1. gcd ($a^{(N-1)/p}$ – 1 , N) = gcd (11^2 – 1 , 263) = 1 is true
   2. $a^{N-1} = 1 \pmod N \Leftrightarrow 11^{262} = 1 \pmod{263}$ is true
   3. F > $\sqrt{N}$
      131 > $\sqrt{263}$ = 16.22 is true
      As all conditions 1, 2 and 3 are true $\Rightarrow$ 263 is prime
2. # of all non-zero elements : 263 – 1 = 262
   # of primitive elements: $\varphi(262) = \varphi(2 * 131) = (2 – 1) * (131 – 1) = 130$
   P(element=primitive) = (130 / 262) * 100 = 49.62%
3. Possible orders are the divisors of 263 – 1 = 263, these are: 1, 2, 131 and 262

   Checking if the element 12 is primitive
   $12^1 \bmod 263 \neq 1$, $12^2 \bmod 263 \neq 1$
   $12^{131} \bmod 263 = 1$ $\Rightarrow$ Ord(12) = 131 $\Rightarrow$ 12 is not a primitive element
   Checking if the element 7 is primitive
   $7^1 \bmod 263 \neq 1$, $7^2 \bmod 263 \neq 1$
   $7^{131} \bmod 263 \neq 1$ $\Rightarrow$ Ord(7) = 262 $\Rightarrow$ 7 is a primitive element

Solution 9-3 cont.:

4. Encryption:

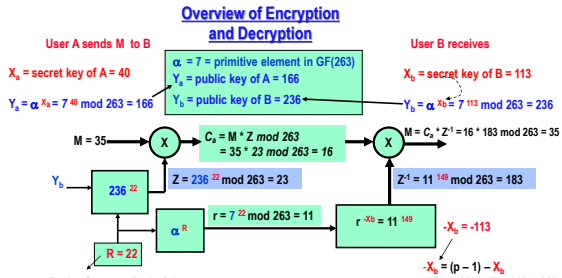


5. Decryption:

$Z^{-1} = r^{-X_b} = 11^{-113 \bmod 262} \bmod 263 = 11^{-113+262} \bmod 263 = 183$
$M = C_a * Z^{-1} = 16 * 183 \bmod 263 = 35$

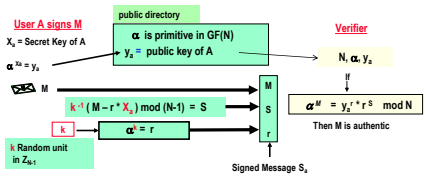
Solution 9-3 cont.:

Overview of Encryption and Decryption



Solution 9-3 cont.:

6.



k has to be invertible mod N-1, N-1 = 262
gcd [k, N-1] = 1 => gcd (121,262) = 1
k = 121, $k^{-1} = 121^{-1} = 13$ (see table below)
$r = \alpha^k = 7^{121} \bmod 263 = 85$

$S = k^{-1} (M – r * X_a) \bmod (N-1)$
$= 121^{-1} (35 – 85 * 113) \bmod 262$
$= 13 (35 – 9605) \bmod 262$
$= -124410 \bmod 262$
S = 40

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE =	
418	13	1	0	0	1	27	13		
15	13	0	1	1	-27	1	2		
13	2	1	-1	-27	28	6	1		
2	1	-1	7	28	-195	2	0	INVERSE=	-195

ElGamal Secrecy-System Over GF (2^m)

Problem 9-4: El-Gamal crypto system is set up using **GF(2^6)**, which is generated by the irreducible polynomial **P(x) = $x^6 + x^5 + x^4 + x^2 + 1 = 1110101$**.

1. Check if you can take **α = 0011** as a primitive element.
2. User A encrypts the message **M = α^3** and send it to user B who has the secret key **X_b = 10** by using the random number **R = 43**. Compute B's public key Y_b and the encrypted message C_a and r.
3. Decrypt the cryptogram C_a on the receiver side B showing all necessary computations therefore.

Note: For the selected P(x), e = 21 this mean ord(x) = 21
(from the table list of all irreducible polynomials over GF(2))

Helping computations :

$x^6 = x^5 + x^4 + x^2 + 1$
$x^7 = x^4 + x^3 + x^2 + x + 1$
$x^8 = x^5 + x^4 + x^3 + x^2 + x$
$x^9 = x^3 + 1$
$x^{10} = x^4 + x$
$x^{11} = x^5 + x^2$
$x^{12} = x^5 + x^4 + x^3 + x^2 + 1$
$x^{16} = x^3 + x^2 + 1$
$x^{21} = 1$

Solution 9-4:

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

Checking if the element α =000011 = x + 1 is primitive

$\alpha^3 = (x+1)^3 = (x+1)^2(x+1) = (x^2+1)(x+1)$
$= x^3 + x^2 + x + 1 \neq 1$
$\alpha^7 = (x+1)^7 = (x+1)^4(x+1)^3 = (x+1)^4(x^3+x^2+x+1)$
$= x^4 + x^2 + 1 \neq 1$
$\alpha^9 = (x+1)^9 = (x+1)^7(x+1)^2$
$= x^5 + x^4 + x^2 \neq 1$
$\alpha^{21} = \alpha^{12} * \alpha^9 = [\alpha^6]^2 * \alpha^9 = (x^5 + x^4 + x^2)^2 = x^{10}(x^5 + x^4 + x^2) = (x^4 + x)(x^5 + x^4 + x^2)$
$= x^4 + x^3 + x^2 + x + 1 \neq 1$
$\Rightarrow$ Ord(α) = 63 $\Rightarrow$ α is a primitive element

Solution 9-4 cont.:

2. Encryption:

User A: $M = \alpha^3$

Public directory: $\alpha = x + 1$, GF(2^6); $Y_b = \alpha^{10}$

User B: $X_b = 10$, $Y_b = \alpha^{X_b} = \alpha^{10}$

Cryptogram:
$C_a = M * Y_b^R = \alpha^3 * (\alpha^{10})^{43}$
$= \alpha^3 * \alpha^{430 \bmod 63} = \alpha^3 * \alpha^{52} = \alpha^{55}$

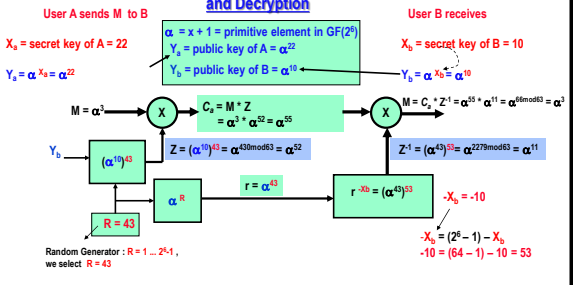
$r = \alpha^R = \alpha^{43}$

3. Decryption:

$Z^{-1} = r^{-X_b} = (\alpha^{43})^{-10 \bmod 63} = (\alpha^{43})^{-10+63} = (\alpha^{43})^{53} = \alpha^{2279 \bmod 63} = \alpha^{11}$
$M = C_a * Z^{-1} = \alpha^{55} * \alpha^{11} = \alpha^{66 \bmod 63} = \alpha^3$

Solution 9-4 cont.:

Overview of Encryption and Decryption



Problem 9-5: El-Gamal crypto system is set up using **GF(2^4)**, which is generated by the irreducible polynomial **P(x) = $x^4 + x + 1 = 10011$**.

1. Compute the exponents of the element δ = x = 000010 as x^i mod P(x) for i= 1 to 15.
2. Which multiplicative orders are possible in **GF(2^4)**?
3. Check if you can take **α = 1011** as a primitive element.
4. User A has the secret key X_a = 7 and User B has the secret key **X_b = 12**. Compute the public keys Y_a and Y_b.
5. User A encrypts the message **M = 0101** and send it to user B by using the random number **R = 13**. Compute the encrypted message C_a and r.
6. Decrypt the cryptogram C_a on the receiver side B showing all necessary computations therefore.

Note: For the selected P(x), e = 15 this mean ord(x) = 15
(from the table list of all irreducible polynomials over GF(2))

Solution 9-5:

1. If $P(x) = x^4 + x + 1$ is the modulus then $x^4 + x + 1 = 0$, thus $x^4 = x + 1$. The exponents of **x** in GF(2^4) are:

$\mathbf{x = x}$	0010	
$\mathbf{x^2 = x^2}$	0100	
$\mathbf{x^3 = x^3}$	1000	
$\mathbf{x^4 = x + 1}$	0011	
$\mathbf{x^5 = x\ x^4 = x^2 + x}$	0110	
$\mathbf{x^6 = x\ (x^2 + x) = x^3 + x^2}$	1100	
$\mathbf{x^7 = x\ (x^3 + x^2) = (x^4 + x^3) = x^3 + x + 1}$	1011	
$\mathbf{x^8 = x^4 + x^2 + x = x + 1 + x^2 + x = x^2 + 1}$	0101	
$\mathbf{x^9 = x^3 + x}$	1010	
$\mathbf{x^{10} = x^4 + x^2 = x^2 + x + 1}$	0111	
$\mathbf{x^{11} = x^3 + x^2 + x}$	1110	
$\mathbf{x^{12} = x^4 + x^3 + x^2 = x^3 + x^2 + x + 1}$	1111	
$\mathbf{x^{13} = x^4 + x^3 + x^2 + x = x^3 + x^2 + 1}$	1101	
$\mathbf{x^{14} = x^4 + x^3 + x = x + 1 + x^3 + x = x^3 + 1}$	1001	
$\mathbf{x^{15} = x^4 + x = x + 1 + x = 1}$	0001	$\Rightarrow$ ord(x) = 15

2. Possible orders are the divisors of $2^4 - 1 = 15$, these are: 1, 3, 5 and 15

Solution 9-5 cont.:

3. Checking if the element $\alpha = 1011 = x^7$ is primitive, ord(x) = 15 (aus 2.)

   $\text{ord}(\alpha) = \text{ord}(x^7) = \text{ord}(x) / \gcd(\text{ord}(x), 7) = 15 / \gcd(15,7) = 15 / 1 = 15$
   $\Rightarrow \text{ord}(\alpha) = 15 \Rightarrow \alpha$ is a primitive element

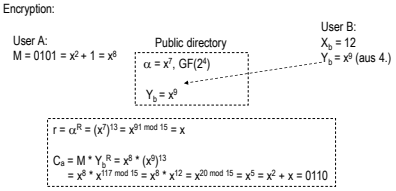
4. $\alpha = 1011 = x^7$

   User A:
   $X_a = 7$
   $Y_a = \alpha^{X_a} = (x^7)^7 = x^{49 \bmod 15} = x^4 = x + 1$
   $= 0011$

   User B:
   $X_b = 12$
   $Y_b = \alpha^{X_b} = (x^7)^{12} = x^{84 \bmod 15} = x^9 = x^3 + x$
   $= 1010$

Solution 9-5 cont.:

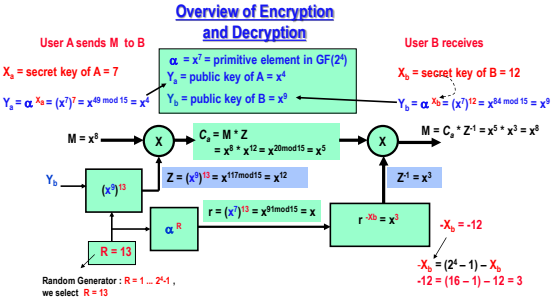
5. Encryption:



6. Decryption:

   $Z^{-1} = r^{-X_b} = x^{-12 \bmod 15} = x^{-12+15} = x^3$
   $M = C_a * Z^{-1} = x^5 * x^3 = x^8 = x^2 + 1 = 0101$

Solution 9-5 cont.:



Problem 9-6:

El-Gamal crypto system is set up using **GF(2^6)**, which is generated by the irreducible polynomial $\mathbf{P(x) = x^6 + x^3 + 1 = 1001001}$.

1. Compute the exponents of the element $\delta = x = 000010$ as $x^i \bmod P(x)$ for i= 1 to 10.
2. Which multiplicative orders are possible in **GF(2^6)**?
3. Compute the probability that a randomly selected element is primitive in **GF(2^6)**.
4. Check if you can take $\boldsymbol{\alpha = x + 1}$ as a primitive element.
5. User A has the secret key $\mathbf{X_a = 22}$ and User B has the secret key $\mathbf{X_b = 10}$. Compute the public keys Y_a and Y_b.
6. User A encrypts the message $\mathbf{M = 100100 = x^5 + x^2}$ and send it to user B by using the random number **R = 20**. Compute the encrypted message C_a and r.
7. Decrypt the cryptogram C_a on the receiver side B showing all necessary computations therefore.

Note: For the selected P(x), e = 9 this mean ord(x) = 9
(from the table list of all irreducible polynomials over GF(2))

Solution 9-6:

1. If $P(x) = x^6 + x^3 + 1$ is the modulus then $x^6 + x^3 + 1 = 0$, thus $x^6 = x^3 + 1$. The exponents of **x** in GF(2^6) are:

$\mathbf{x = x}$	000010	
$\mathbf{x^2 = x^2}$	000100	
$\mathbf{x^3 = x^3}$	001000	
$\mathbf{x^4 = x^4}$	010000	
$\mathbf{x^5 = x^5}$	100000	
$\mathbf{x^6 = x^3 + 1}$	001001	
$\mathbf{x^7 = x\ (x^3 + 1) = x^4 + x}$	010010	
$\mathbf{x^8 = x^5 + x^2}$	100100	
$\mathbf{x^9 = x^6 + x^3 = x^3 + 1 + x^3 = 1}$	000001	$\Rightarrow$ ord(x) = 9 $\Rightarrow$ x is not primitive
$\mathbf{x^{10} = x}$	000010	

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

3. # of all non-zero elements: $2^6 - 1 = 63$
   # of primitive elements: $\varphi(63) = \varphi(3^2 * 7) = 63 * (1 - 1/3) * (1 - 1/7) = 36$

   P(element = primitive) = (36 / 63) * 100 = 57.14%

Solution 9-6 cont.:

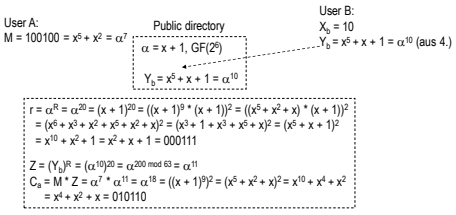
4. Checking if the element $\alpha = x + 1$ is primitive

$x + 1 \neq 1$
$(x+1)^3 = (x+1)^2 * (x+1) = (x^2+1)(x+1) = \mathbf{x^3 + x^2 + x + 1 \neq 1}$
$(x+1)^6 = ((x+1)^3)^2 = (x^3+x^2+x+1)^2 = x^6 + x^4 + x^2 + 1 = x^3 + 1 + x^4 + x^2 + 1 = \mathbf{x^4 + x^3 + x^2}$
$(x+1)^7 = (x+1)^6 * (x+1) = (x^4 + x^3 + x^2)(x+1) = x^5 + x^4 + x^3 + x^4 + x^3 + x^2 = \mathbf{x^5 + x^2 \neq 1}$
$(x+1)^9 = (x+1)^7 * (x+1)^2 = (x^5 + x^2)(x^2+1) = x^7 + x^5 + x^4 + x^2 = x^4 + x + x^5 + x^4 + x^2 = \mathbf{x^5 + x^2 + x \neq 1}$
$(x+1)^{21} = ((x+1)^7)^3 = (x^5 + x^2)^2 * (x^5 + x^2) = (x^{10} + x^4) * (x^5 + x^2) = (x^4 + x) * (x^5 + x^2) = x^9 + x^6 + x^5 + x^3$
$= \mathbf{x^3 + 1 \neq 1}$
$\Rightarrow$ ord(α) = 63 $\Rightarrow$ α is a primitive element

5. $\alpha = x + 1$
User A:
$X_a = 22$
$Y_a = \alpha^{Xa} = (x+1)^{22} = (x+1)^{21} * (x+1) = (x^3+1)(x+1) = x^4 + x + x^3 + 1 = x^4 + x^3 + x + 1 = 011011$
User B:
$X_b = 10$
$Y_b = \alpha^{Xb} = (x+1)^{10} = (x+1)^9 * (x+1) = (x^5 + x^2 + x)(x+1) = x^6 + x^3 + x^2 + x^5 + x^2 + x = x^3 + 1 + x^3 + x^5 + x$
$= x^5 + x + 1 = 100011$

Solution 9-6 cont.:

6. Encryption:



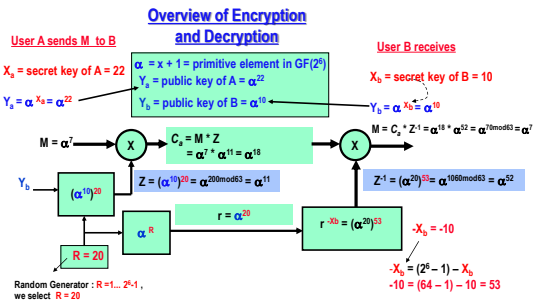
$r = \alpha^R = \alpha^{20} = (x+1)^{20} = ((x+1)^9 * (x+1))^2 = ((x^5 + x^2 + x) * (x+1))^2$
$= (x^6 + x^3 + x^2 + x^5 + x^2 + x)^2 = (x^3 + 1 + x^3 + x^5 + x)^2 = (x^5 + x + 1)^2$
$= x^{10} + x^2 + 1 = x^2 + x + 1 = 000111$

$Z = (Y_b)^R = (\alpha^{10})^{20} = \alpha^{200 \bmod 63} = \alpha^{11}$
$C_a = M * Z = \alpha^7 * \alpha^{11} = \alpha^{18} = ((x+1)^9)^2 = (x^5 + x^2 + x)^2 = x^{10} + x^4 + x^2$
$= x^4 + x^2 + x = 010110$

7. Decryption:

$Z^{-1} = r^{-Xb} (\alpha^{20})^{-10} = \alpha^{-200 \bmod 63} = \alpha^{-11} = \alpha^{52}$
$M = C_a * Z^{-1} = \alpha^{18} * \alpha^{52} = \alpha^{70 \bmod 63} = \alpha^7 = x^5 + x^2 = 100100$

Solution 9-6 cont.:



Problem 9-7: El-Gamal crypto system is set up using **GF(2^8)**, which is generated by the irreducible polynomial **$P(x) = x^8 + x^5 + x^4 + x^3 + 1 = 100111001$**.

1. Compute the exponents of the element $\delta = x = 000010$ as x^i mod P(x) for i= 1 to 17.
2. Which multiplicative orders are possible in **GF(2^8)**?
3. Check if you can take **$\alpha = 1011$** as a primitive element.
4. User A has the secret key **$X_a = 101$** and User B has the secret key **$X_b = 42$**. Compute the public keys Y_a and Y_b (the form α^x is sufficient).
5. User A encrypts the message **$M = \alpha^4$** and send it to user B by using the random number **R = 91**. Compute the encrypted message C_a and r (the form α^x is sufficient)..
6. Decrypt the cryptogram C_a on the receiver side B showing all necessary computations therefore (the form α^x is sufficient).

Note: For the selected P(x), e = 17 this mean ord(x) = 17
(from the table list of all irreducible polynomials over GF(2))

Helping computations :
$(x+1)^{25} = x^7 + x^6 + x$
$(x+1)^{80} = x^7 + x^6 + x^3 + 1$

Solution 9-7:

1. If $P(x) = x^8 + x^5 + x^4 + x^3 + 1$ is the modulus then $x^8 + x^5 + x^4 + x^3 + 1 = 0$,
thus $x^8 = x^5 + x^4 + x^3 + 1$. The exponents of **x** in GF(2^8) are:

$\mathbf{x = x}$	00000010
$\mathbf{x^2 = x^2}$	00000100
$\mathbf{x^3 = x^3}$	00001000
$\mathbf{x^4 = x^4}$	00010000
$\mathbf{x^5 = x^5}$	00100000
$\mathbf{x^6 = x^6}$	01000000
$\mathbf{x^7 = x^7}$	10000000
$\mathbf{x^8 = x^5 + x^4 + x^3 + 1}$	00111001
$\mathbf{x^9 = x^6 + x^5 + x^4 + x}$	01110010
$\mathbf{x^{10} = x^7 + x^6 + x^5 + x^2}$	11100100
$\mathbf{x^{11} = x^8 + x^7 + x^6 + x^3 = x^7 + x^6 + x^5 + x^4 + 1}$	11110001
$\mathbf{x^{12} = x^8 + x^7 + x^6 + x^5 + x = x^7 + x^6 + x^4 + x^3 + x + 1}$	11011011
$\mathbf{x^{13} = x^8 + x^7 + x^5 + x^4 + x^2 + x = x^7 + x^3 + x^2 + x + 1}$	10001111
$\mathbf{x^{14} = x^8 + x^4 + x^3 + x^2 + x = x^5 + x^2 + x + 1}$	00100111
$\mathbf{x^{15} = x^6 + x^3 + x^2 + x}$	01001110
$\mathbf{x^{16} = x^7 + x^4 + x^3 + x^2}$	10011100
$\mathbf{x^{17} = x^8 + x^5 + x^4 + x^3 = 1}$	00000001 $\Rightarrow$ ord(x) = 17 $\Rightarrow$ x is not primitive

Solution 9-7 cont.:

2. Possible orders are the divisors of $2^8 – 1 = 255$, these are: 1, 3, 5, 15, 17, 51, 85 and 255

3. Checking if the element $\alpha = 00000011 = x + 1$ is primitive
$x + 1 \neq 1$
$(x+1)^3 = (x+1)^2 * (x+1) = (x^2+1)(x+1) = \mathbf{x^3 + x^2 + x + 1 \neq 1}$
$(x+1)^5 = (x+1)^3 * (x+1)^2 = (x^2+1)(x^3+x^2+x+1) = x^5 + x^4 + x^3 + x^2 + x^3 + x^2 + x + 1 = \mathbf{x^5 + x^4 + x + 1 \neq 1}$
$(x+1)^{15} = ((x+1)^5)^3 = (x^5 + x^4 + x + 1)^2 * (x^5 + x^4 + x + 1) = (x^{10} + x^8 + x^2 + 1) * (x^5 + x^4 + x + 1)$
$= (x^7 + x^6 + x^5 + x^2 + x^5 + x^4 + x^3 + 1 + x^2 + 1) * (x^5 + x^4 + x + 1) = (x^7 + x^6 + x^4 + x^3) * (x^5 + x^4 + x + 1)$
$= x^{12} + x^{11} + x^6 + x^7 + x^{11} + x^{10} + x^7 + x^6 + x^8 + x^6 + x^5 + x^4 + x^8 + x^7 + x^4 + x^3$
$= x^{12} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^3$
$= x^7 + x^6 + x^4 + x^3 + x + 1 + x^7 + x^6 + x^5 + x^2 + x^6 + x^5 + x^4 + x + x^5 + x^4 + x^3 + 1 + x^7 + x^6 + x^5 + x^3$
$= \mathbf{x^7 + x^4 + x^3 + x^2 \neq 1}$
$(x+1)^{17} = (x+1)^{15} * (x+1)^2 = (x^7 + x^4 + x^3 + x^2)(x^2 + 1) = x^9 + x^6 + x^5 + x^4 + x^7 + x^4 + x^3 + x^2$
$= x^6 + x^5 + x^4 + x + x^6 + x^5 + x^4 + x^7 + x^4 + x^3 + x^2 = \mathbf{x^7 + x^4 + x^3 + x^2 + x \neq 1}$
$(x+1)^{51} = ((x+1)^{25})^2 * (x+1) = (x^7 + x^6 + x)^2 * (x+1) = (x^{14} + x^{12} + x^2) * (x+1) = x^{15} + x^{13} + x^3 + x^{14} + x^{12} + x^2$
$= x^6 + x^3 + x^2 + x + x^7 + x^3 + x^2 + x + 1 + x^3 + x^5 + x^2 + x + 1 + x^7 + x^6 + x^4 + x^3 + x + 1 + x^2$
$= \mathbf{x^5 + x^4 + 1 \neq 1}$
$(x+1)^{85} = (x+1)^{80} * (x+1)^5 = (x^7 + x^6 + x^3 + 1)(x^5 + x^4 + x + 1)$
$= x^{12} + x^{11} + x^8 + x^5 + x^{11} + x^{10} + x^7 + x^6 + x^8 + x^7 + x^4 + x + x^7 + x^6 + x^3 + 1 = x^{12} + x^{10} + x^7 + x^5 + x^4 + x^3 + x + 1$
$= x^7 + x^6 + x^4 + x^3 + x + 1 + x^7 + x^6 + x^5 + x^2 + x^7 + x^5 + x^4 + x^3 + x + 1 = \mathbf{x^7 + x^2 \neq 1}$
$\Rightarrow$ ord(α) = 255 $\Rightarrow$ α is a primitive element

Solution 9-7 cont.:

4. $\alpha = x + 1$

User A: $X_a = 101$, $Y_a = \alpha^{X_a} = \alpha^{101}$

User B: $X_b = 42$, $Y_b = \alpha^{X_b} = \alpha^{42}$

5. Encryption:

User A: $M = \alpha^4$

Public directory: $\alpha = x + 1$, $GF(2^8)$; $Y_b = \alpha^{42}$

User B: $X_b = 42$; $Y_b = \alpha^{42}$ (aus 4.)

Encryption:

$r = \alpha^R = \alpha^{91}$

$C_a = M * Y_b^R = \alpha^4 * (\alpha^{42})^{91} = \alpha^4 * \alpha^{3822 \bmod 255} = \alpha^4 * \alpha^{252}$
$= \alpha^{256 \bmod 255} = \alpha$

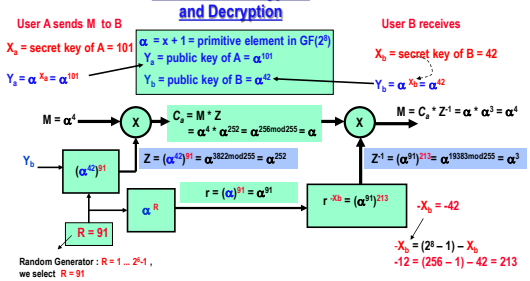
6. Decryption:

$Z^{-1} = r^{-X_b} = (\alpha^{91})^{-42} = \alpha^{-3822 \bmod 255} = \alpha^3$

$M = C_a * Z^{-1} = \alpha * \alpha^3 = \alpha^4$

Solution 9-7 cont.:

Overview of Encryption and Decryption



Online ad-hoc
Interactive Examples

Online Tutorial 1. 30.03.2021:

ElGamal crypto system is set up, use the element $\alpha = 35$ as a public element and compute the DH public keys Y_a and Y_b for users A and B having the secret keys $X_a = 21$ und $X_b = 29$.

1- Generate a prime number by using Pocklington Theorem:

$N = FR + 1$

$N = 2^*(41) + 1 = 83$, $F = 41$ and $R = 2$

83 is a prime if all the following conditions hold :

Proof: select $a = 2$ ($1 < a < 83$) remark a is an integer prime to N

1. $a^{n-1} \equiv 1 \pmod n$
   $2^{83-1} = 1 \mod 83$ (or in Z_{83}) is true

2. $\gcd(a^{(n-1)/qi} - 1, n) = 1$
   $\gcd(2^{(83-1)/41} - 1, 83) = \gcd(2^2 - 1, 83) = \gcd(4,83) = 1$ is true

3. $F = 41 > \sqrt{83}$ => $41 > 9.11$ is true

As all conditions hold, => p=83 is for sure a prime

3- Compute and verify the Signature S_a according to ElGamal signature scheme for the same message M=60

User A signs M

$X_a = 21$

$Y_a = \alpha^{X_a} = 35^{21} \bmod 83$

$\alpha = 35$ primitive element in GF(83)
$Y_a = \alpha^{X_a} = 52$
$Y_b = \alpha^{X_b} = 80$

Verifier

$X_b = 29$

$Y_b = \alpha^{X_b} = 35^{29} \bmod 83$

Message to be signed by A: M = 60

$k^{-1}(M - r \cdot X_a) \bmod (N-1) = S$
$73(60 - 73.21) \bmod 82 = 55$

M = 60
S = 55
r = 73

K = 9 → $\alpha^K \bmod P = r$
$35^9 \bmod 83 = 73$

k Random unit in Z_{N-1}

$\alpha^M \bmod p = (Y_a)^r \cdot r^S \bmod p$

$(35)^{60} \bmod 83 = (52)^{73} \cdot (73)^{55} \bmod 83$
$69 = 69$
=> That is M is authentic

Signed Message S_a

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE = B2		GCD	
82	9	1	0	0	1	9	1				
9	1	0	1	1	-9	9	0	INVERSE=	-9	GCD=	1

2- Compute the ElGamal cryptogram CA using GF(83) for the message M=60 sent from A to B using a random R=9.

User A sends M to B

$X_a = 21$
$Y_a = \alpha^{X_a} = 35^{21} \bmod 83$

$\alpha = 35$ primitive element in GF(83)
$y_a = \alpha^{X_a} = 52$
$y_b = \alpha^{X_b} = 80$

User B receives

Xb = 29
$y_b = \beta^{X_b} = 35^{29} \bmod 83$

M = 60 → X → C = M.Z mod P= 60.71 mod 83= 27 → X → M

M=C . Z^{-1}
=27.76 mod 83 = 60 = M

$Z = (Y_b)^R \bmod p = (80)^9 \bmod 83 = 71$

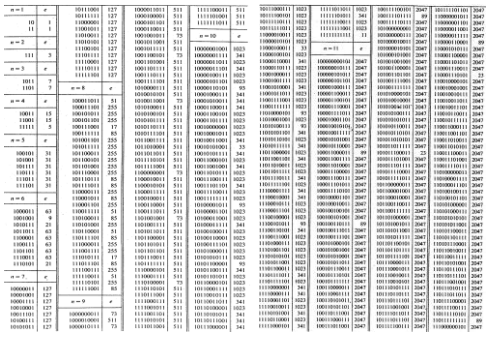
$r = \alpha^R \bmod p = (35)^9 \bmod 83 = 73$

$Z^{-1} = (r)^{X_b} = 73^{53} \bmod 83 = 76$

With $+X_b = -Xb + p-1$
$+X_b = -29 + 82 = 53$

R = 9

Annex: List of all irreducible Polynomials over GF(2) up to degree 11



Annex: Some factorizations for 2^n-1

$2^3 - 1 = 7$

$2^4 - 1 = 3 \times 5$

$2^5 - 1 = 31$

$2^6 - 1 = 3 \times 3 \times 7$

$2^7 - 1 = 127$

$2^8 - 1 = 3 \times 5 \times 17$

$2^9 - 1 = 7 \times 73$

$2^{10} - 1 = 3 \times 11 \times 31$

$2^{11} - 1 = 23 \times 89$

$2^{12} - 1 = 3 \times 3 \times 5 \times 7 \times 13$

$2^{13} - 1 = 8191$

$2^{14} - 1 = 3 \times 43 \times 127$

$2^{15} - 1 = 7 \times 31 \times 151$

$2^{16} - 1 = 3 \times 5 \times 17 \times 257$

$2^{17} - 1 = 131071$

$2^{18} - 1 = 3 \times 3 \times 3 \times 7 \times 19 \times 73$

$2^{19} - 1 = 524287$

$2^{20} - 1 = 3 \times 5 \times 5 \times 11 \times 31 \times 41$

$2^{21} - 1 = 7 \times 7 \times 127 \times 337$

$2^{22} - 1 = 3 \times 23 \times 89 \times 683$

$2^{23} - 1 = 47 \times 178481$

$2^{24} - 1 = 3 \times 3 \times 5 \times 7 \times 13 \times 17 \times 241$

$2^{25} - 1 = 31 \times 601 \times 1801$

$2^{26} - 1 = 3 \times 2731 \times 8191$

$2^{27} - 1 = 7 \times 73 \times 262657$

$2^{28} - 1 = 3 \times 5 \times 29 \times 43 \times 113 \times 127$

$2^{29} - 1 = 233 \times 1103 \times 2089$

$2^{30} - 1 = 3 \times 3 \times 7 \times 11 \times 31 \times 151 \times 331$

$2^{31} - 1 = 2147483647$

$2^{32} - 1 = 3 \times 5 \times 17 \times 257 \times 65537$

$2^{33} - 1 = 7 \times 23 \times 89 \times 599479$

$2^{34} - 1 = 3 \times 43691 \times 131071$