Introduction to Cryptology

Tutorial-10
Rabin Lock for Public-Key Systems

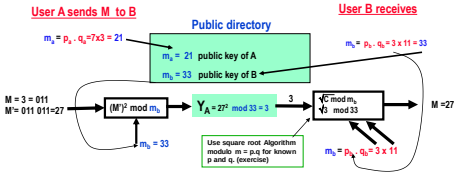
17.05.2023, v40

Problem 10-1:

1. Set up a Rabin Pubic-Key secrecy system using for user A and B the prime numbers 7,3 and 11,3 respectively
2. User A Encrypts the message M=3 to get the cryptogram Y_A and sends it to B
3. Let user B decrypt the cryptogram Y_A

Solution 10-1:

Set up and calculate Cryptogram and decrypt the message M=3 for a user with the public key m_b = 3x11=33



Solution Cont.: See square root algorithm calculations:

Decryption:
Take p = 11, q = 3, and n = 33.
Then gcd(11,3) = (-1)*11 + (4)*3 = 1, so that **a = -1** and **b = 4**.

To decrypt compute the square root of C modulo 33:
r = $c^{(p+1)/4}$ mod p => r = 3^3 mod 11 = 5
s = $c^{(q+1)/4}$ mod q => s = 3^1 mod 3 = 0
And
x = (a*p*s + b*q*r) mod m => x = ((-1)*11*0 + 4*3*5) mod 33 = **27**
y = (a*p*s - b*q*r) mod m => y = ((-1)*11*0 - 4*3*5) mod 33 = **6**

These are two of the four square roots, and the remaining two are
-x mod 33 = -27 mod 33 = **6**
-y mod 33 = -6 mod 33 = **27**

In binary, the four square roots are
27 = 011011
6 = 000110
6 = 000110
27 = 011011

The only sqare root with two equal halfs Is the correct result

One of these roots is M'. Only 27 has the required repetition redundancy, so this is the only possible message **M'= 27 =** 011011 => **M = 011**.

Problem 10-2:

1. Two square roots are somehow found in $\mathbf{Z}_m$ in the following cases:

1 - √	25	= 5 and	31	mod 39
2- √	66	= 41 and	24	mod 85
3 - √	54	= 33 and	36	mod 69

Try to factorize **m = p .q** in all cases.
Hint: gcd [m, (a+b)] = p or q and roots a and b are distinct, that is a≠-b and a≠b (1)

Solution 10-2:

1- Check: As 31 ≠ -5 ≠ 5 mod 39 , therefore factorization according to (1)
That is gcd (39, (31 + 5)) = 3=p is one of the factors. q = 39/3=13

2- Check: As 41 ≠ -24 ≠ 24 mod 85 , therefore factorization according to (1)
That is gcd (85, (41 + 24)) = 5 =p is one of the factors. q = 85/5=17

3- Check: as 33=-36 mod 69, factorization is not computable.

Problem 10-3: Rabin Signature Scheme

n = p .q = 713 is public, p =23 and q = 31 are two secret primes

The message m = 14 is to be signed. The hash function is *H(m) = (2m³ + 3m²) mod 547* = 59

If: $H(m)^{\frac{p-1}{2}} \bmod p = 1$ **AND** $H(m)^{\frac{q-1}{2}} \bmod q = 1$ **Is true**

The signature S is :

$$S = \left(\left(p^{q-2} H(m)^{\frac{q+1}{4}} \bmod q \right) p + \left(q^{p-2} H(m)^{\frac{p+1}{4}} \bmod p \right) q \right) \bmod (p \cdot q)$$

S = [(23^{29} 59^8 mod 31) 23 + (31^{21} 59^6 mod 23) 31] mod 713
S = [(13) 23 + (18) 31] mod 713 = 144

Verification
Check if: $H(m) = S^2 \bmod (p \cdot q)$
59 = 144^2 mod 713 = 59

Problem 10-4: Rabin Pubic-Key Secrecy System (Exam 2019)

1. **Set up a Rabin pubic-key secrecy system for user A and B by deploying the prime numbers 7, 13 and 19,11 respectively as secret keys.**
2. **User A encrypts the message M = 15 as a clear text using a tag T . That is M' = 15||T is encrypted to get the cryptogram Y_A and sends it to B. Compute Y_A assuming that the selected tag T = 3 is known to both sender and receiver.**
   (|| means concatenation of bit streams)
3. **Let user B decrypt the cryptogram Y_A showing all necessary computations**
4. **Is it necessary to select an alternative tag T to decrypt Y_A correctly? Why?**

Solution

1. Rabin pubic-key secrecy system

User A sends M to B

$m_a = p_a \cdot q_a = 7 \times 13 = 91$

Public directory

$m_a = 91$

$m_b = 209$

User B receives

$m_b = p_b \cdot q_b = 19 \times 11 = 209$

2. A Encrypts M'= M||T=15||3

M'= M || T = 15||3

M'= 1111011=123

$(M')^2 \bmod m_b$ → $Y_A = 123^2 \bmod 209 = 81$ → $\sqrt{81} \bmod 209$ (81)

3. To compute the square root M':

Take p = 19, q = 11, and m = 209.

Then gcd(11,5) = (-4)*19 + (7)*11 = 1, that is **a = -4** and **b = 7**

m	u	a1	a2	b1	b2	q	r	INVERSE VALUE = B2		GCD	
19	11	1	0	0	1	1	8				
11	8	0	1	1	-1	1	3				
8	3	1	-1	-1	2	2	2				
3	2	-1	3	2	-5	1	1				
2	1	3	-4	-5	7	2	0	NVERSE=	7	GCD=	1

Solution

To decrypt, compute the square root of C=81 modulo 209:

$r = c^{(p+1)/4} \bmod p \Rightarrow r = 81^5 \bmod 19 = 9$

$s = c^{(q+1)/4} \bmod q \Rightarrow s = 81^3 \bmod 11 = 9$

And

$x = (a*p*s + b*q*r) \bmod m \Rightarrow x = ((-4)*19*9 + 7*11*9) \bmod 209 = 9$

$y = (a*p*s - b*q*r) \bmod m \Rightarrow y = ((-4)*11*9 + 7*11*9) \bmod 209 = 86$

These are two of the four square roots, and the remaining two are

-x mod 209 = -9 mod 209 = 200

-y mod 209 = -86 mod 209 = 123

In binary, the four square roots are

9 = 00001001_2

86 = 01010110_2

200 = 11001000_2

123 = 01111011_2

The only root that contians the predefined tag T=3=011

Therefore, the correct Message decryption is 123 = 01111 011

The correct clear text message M =01111=15.

4. No need to repeat with a new tag, as the result was unique .