### WEB3CLUBS FOUNDATION LIMITED

Course Instructor: DR. Cyprian Omukhwaya Sakwa

PHONE: +254723584205 Email: cypriansakwa@gmail.com

### Foundational Mathematics for Web3 Builders

Lecture 22
June 10, 2024

# **RSA** Digital Signature Algorithm

The RSA Digital Signature Algorithm is comparable to the RSA algorithm.

### Algorithm 1

Assume that you intend to sign and send a message n to your friend. You do the following:

- 1. Select two prime numbers p and q such that  $p \neq q$  and calculates  $m = p \times q$ .
  - Note that m will be made public while p and q will be kept private.
- 2. Calculate  $\phi(m) = (p-1)(q-1)$
- 3. Choose an integer e such that,  $1 < e < \phi(m)$  and e is coprime to  $\phi(m)$ .

Note that e will be made public.  $\boldsymbol{\mathcal{C}}$ 

# Algorithm (conti...)

- 5. Compute the d such that,  $1 < d < \phi(m)$  and that  $ed \equiv 1 \pmod{\phi(m)}$ . Note that d will be private.
- 6. Publishe the public key (m,e) and keeps  $p,q,\bar{d}$  and  $\phi(m)$  private.
- 7. Create your signature by raising n to the power d modulo m.
- - 8. Send n and s to your friend. That is, send the signed ducument (n,s).
  - 9. Your friend verifies that it is really you who signed the message by using your public key (m,e) then raises s to the power e modulo m.

$$s^e = (n^l)^e = s^e \equiv (n^d)^e \equiv n^{ed} \equiv n \mod m$$

As a result, nobody should be able to forge your signature. If a document has your signature, you cannot successfully deny signing it.

### Example 1

For each of the following, show how Ken would sign a message m using RSA digital signature algorithm with modulus  $n=p\times q$  to obtain a signed document (m,s) if he chooses a public exponent e. Then show how Naomi would verify that the message was signed by Ken.

a) 
$$p = 5$$
,  $q = 13$ ,  $e = 7$ ,  $m = 6$ 

b) 
$$p = 7$$
,  $q = 19$ ,  $e = 5$   $m = 7$ 

$$n = P_{\gamma} = 65$$
  
 $\phi(n) = (5-1)(13-1) = 48$   
 $e = 7 \text{ HW} 7^{1} \text{ mod } 48 = 3$ 

a) Here,  $n = 5 \times 13 = 65$  and  $\phi(n) = 4 \times 12 = 48$ .

Now find d such that  $7d \equiv 1 \mod 48$ . By Euclid's algorithm

we have

$$48 = 7(6) + 6$$

$$7 = 6(1) + 1$$

$$6 = 1(6) + 0$$

Now use extended Euclidean algorithm to get

$$1 = 7 - 6(1) = 7 - [48 - 7(6)](1)$$

$$= 7 - 48(1) + 7(6) = 7(7) + 48(-1)$$

Thus d=7. The public key is (65,7) and private key is (65,7)

To sign the private key is used.

Signature:  $s = m^d = 6^7 \mod 65 = 46 \mod 65$ .

Signed document is (m,s)=(6,46)

To verify we use the public keeps used.

279936 mad 6



 $(46^7)$  mod 65. Let us use the fast powering algorithm.

$$46^1 = 46$$

$$46^2 = 36$$

$$46^4 = 61$$

$$\therefore 46^7 = 46^4 \times 46^2 \times 46^1 \checkmark$$

$$=61 \times 36 \times 46 = 6$$

Hence verified.

b) Here,  $n = 7 \times 19 = 133$  and  $\phi(n) = 6 \times 18 = 108$ .

By Euclid's algorithm we get: (7-1) (17-1)

Now find d such that  $5d \equiv 1 \mod 108$ 

$$108 = 5(21) + 3$$

$$5 = 3(1) + 2$$

$$3 = 2(1) + 1$$

Now use extended Euclidean algorithm

$$1 = 3 - 2(1) = 3 - [5 - 3(1)](1)$$

$$= 3 - 5(1) + 3(1) = 5(-1) + 3(2)$$

$$= 5(-1) + [108 - 5(21)](2) = 108(2) + 5(-43)$$

Thus,  $d = -43 \mod 108 \equiv 65$ 

Signature:  $s \neq 7^{65} \mod 133$ .

Use fast powering algorithm

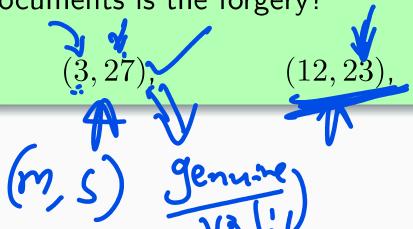
$$7^{1} = 7$$
 $7^{4} = 7$ 
 $7^{8} = 49$ 
 $7^{16} = 7$ 
 $7^{16} = 7$ 
 $7^{16} = 7$ 
 $7^{16} = 7$ 
 $7^{16} = 7$ 
 $7^{16} = 7$ 
 $7^{16} = 7$ 
 $7^{16} = 7$ 
 $7^{16} = 7$ 
 $7^{16} = 7$ 
 $7^{16} = 7$ 

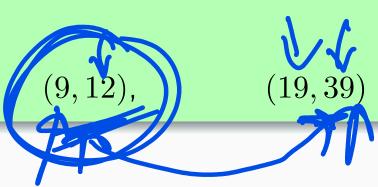
Thus signed document is (7,49)

To verify we compute  $49^5 \mod 133 = 7$ 

# Example 2

Lynette uses the RSA signature with public modulus 55 and public encryption exponent 7. She then sends three documents to Alex with her signature attached. Alex creates a fourth document and unsuccessfully tries to forge Alice's signature. Which of the four documents is the forgery?





(55,7)

$$S=23$$
  
 $S^{3}=23^{7}$  mi)  $55=12$   
 $61905917.2$ 

(3) 
$$S=12$$

$$S^{7}=12^{7} \text{mod} S5=23$$

$$651,487.418$$

### Example 3

Cyprian chooses primes p=113 and q=167 and public exponent e=71. He wants to sign the document m=11. What is the signed document? Show the calculations that verify that the above signed document is valid.

#### Solution

 $n = 113 \times 167 = 18871$  and  $\phi(n) = 112 \times 166 = 18592$ 

Now find d if  $71d \equiv 1 \mod 18592$ 

By Euclid's algorithm we have

$$18592 = 71(261) + 61$$
$$71 = 61(1) + 10$$
$$61 = 10(6) + 1$$

By extended Euclidean algorithm we have

$$1 = 61 - 10(6) = 61 - [71 - 61(1)](6)$$

$$= -71(6) + 61(7) = -71(6) + [18592 - 71(261)](7)$$

$$= 18592(7) + 71(-1833)$$

Thus  $d = -1833 \mod 18592 = 16759$ 

The signature  $s=11^{16759} \bmod 18871=2321$  by fast powering algorithm

The signed document is (11, 2321)

To verify we compute  $2321^{71} \bmod 18871 = 11$  by fast powering algorithm

### Exercise (conti...)

- 3. Alex chooses 7 and 11 as p and q and calculates  $n=7\times 11=77$ . The value of  $\phi(n)=(7-1)(11-1)=60$ . If he chooses e=23 to be his public key, calculate d, his private key such that  $ed\equiv 1 \bmod \phi(n)$ . Now imagine that Wanjiru wants to send the plaintext 15 to Alex. Show how Wanjiru would encrypt 15 and how Alex would decrypt the ciphertext.
- 4. Now assume that Ochieng' wants to send a message to Alex. Ochieng' can use the same public key announced by Alex (probably on his website), 23; Ochieng''s plaintext is 67. Show how Ochieng' would encrypt 67 and how Alex would decrypt the ciphertext.

### Exercise (Conti...)

5. You have been sent the following message. You may use your computer.

79880, 113612, 97518, 82767, 80745, 102524, 1076, 102745, 91940

It has been encrypted using p=313, q=373, m=pq=116749, and e=161. Decrypt the message.

- 6. Encrypt "YOU SETTLE THE CASE" using p=5, q=17, e=3. How will your friend decrypt the ciphertext?
- 7. Write a program to implement the RSA cryptosystem. Make your program as user friendly as possible. In particular, the person encoding a message should be able to type in their message as words, including spaces and punctuation; similarly, the decoder should see the message appear as words with spaces and punctuation decrypt this?

16/15

### Exercise (Conti...)

- 8 Lynette has public RSA modulus  $n=119=7\times 17$  and public exponent e=5. She wants to sign the document m=7.
  - a) What is the signed document?
  - b) Show that Alex calculation verifies that the document you produced in part (a) is valid.