WEB3CLUBS FOUNDATION LIMITED

Course Instructor: DR. Cyprian Omukhwaya Sakwa
PHONE: +254723584205 Email: cypriansakwa@gmail.com

Foundational Mathematics for Web3 Builders

Lecture 10

May 13, 2024

1.1 Cryptanalysis of RSA

RSA algorithm relies that p and q, the distinct prime numbers, are kept secret, even though $m = p \times q$ is made public.

The reason prime numbers are fundamental to RSA encryption is because when you multiply two together, the result is a number that can only be broken down into those primes (or itself and a 1).

When you use much larger prime numbers for your p and q, it's pretty much impossible for computers to nut them out from m. If m is an extremely large number, the problem reduces to find the factors that make up the number m, which is known as the factorization attack.

Note that there is no known way of cracking the RSA system without essentially factoring m and hence the security of the RSA system depends on the difficulty of factoring n

1.2 Factorization Attack

Recall that the security of RSA is based on the idea that the modulus is so large that it is infeasible to factor it in a reasonable time.

If the middleman, Eve, can factor m correctly, then she correctly guesses p, q and calculates $\phi(m) = (p-1)(q-1)$.

Since the public key e is public, Eve can compute the multiplicative inverse of e to find d. That is,

$$d = e^{-1} \bmod \phi(m).$$

She can then use d to decrypt any encrypted message.

But if the modulus m was chosen to be 1024 bits long, it would take considerable time to break the RSA system unless an efficient factorization algorithm could be found.

1.3 Chosen Ciphertext Attack

Here, an attacker chooses ciphertext messages and gets decryption assistance to obtain the corresponding plaintext messages.

How it works

Suppose I encrypt a message p using the public key e of Alex and send the encrypted message c to Alex.

$$c = \boxed{p^e} \bmod m$$

Suppose also that the intruder Eve intercepts the message and manipulates the message before forwarding to Alex.

1. Eve chooses a random integer $x \in \mathbb{Z}_m^*$ (i.e a number relatively prime to m since m is public).
2. Eve calculates $\underline{y} = \boxed{c \times x^e} \pmod m$ and sends y to Alex.

How it works (conti...)

3. Alex decrypts y using his private key d.

$$z = y^d \pmod m.$$

4. Eve can discover the plaintext p as follows:

$$\begin{aligned} z = y^d \pmod m &= (c \times x^e)^d \pmod m \\ &= \left(c^d \times x^{ed}\right) \pmod m \\ &= \left(c^d \times x\right) \pmod m \end{aligned}$$

Thus $z = p \times x \pmod m$

Eve can now use the Extended Euclidean algorithm to compute x^{-1} and obtain p as

$$p = z \times x^{-1} \pmod m$$

1.4 Digital Signatures

Let us suppose Lynette applies for insurance. She calls up her broker, Ken, they negotiate, and Ken sends her a printed contract in an envelope via mail. Lynette would then read it, sign it, and mail it back to Ken. However, this process may take more days and has cost implications (paper, ink, and postage) to both Lynette and Ken.

Ken may also choose the option of sending this contract via e-mail and have Lynette approve it, saving them both time and money. He may not have to worry about encrypting the document since nothing secretive about it. But what guarantee does he have that the person who approves and signs it is really Lynette? Maybe it's someone else in her household with access to her e-mail account or maybe it's Lynette's enemy who masquerades electronically as Lynette.

There are several methods that can be used to guarantee that Lynette's response is as legally binding as a written signature. Let us discuss one that allows a digital signature to be attached to a message using RSA-type techniques.

How it works:

1. Let us call the insurance policy that Ken has written for Lynette n.
2. Lynette Selects two prime numbers p and q such that $p \neq q$ and calculates $m = p \times q$.

   Note that m will be a public key while p and q will be kept private.
3. Lynette calculates $\phi(m) = (p-1)(q-1)$
4. Lynette chooses an integer e such that, $1 < e < \phi(m)$ and e is coprime to $\phi(m)$.

   Note that e will be another public key.

5. Lynette computes the d such that, $1 < d < \phi(m)$ and that $ed \equiv 1 (\mathrm{mod}\, \phi(m))$.

   Note that d will be a private key.

6. Lynette publishes the public key (m, e) and keeps p, q, d and $\phi(m)$ private.

7. After reading the insurance policy, Lynette creates her signature by raising n to the power d modulo m.

   Lynette's Signature: $s \equiv n^d \bmod m$

8. Lynette sends n and s to Ken. That is, she sends the signed ducument (n, s).

9. Ken Verifies that it's really Lynette who has agreed to the contract by using Lynette's public key (m, e) then raises s to the power e modulo m.

$$s^e \equiv (n^d)^e \equiv n^{ed} \equiv n \bmod m$$

As a result, no one should be able to forge Lynette's signature. Therefore, if a document is signed with Lynette's signature, Lynette cannot successfully deny that she signed it.

Exercise 1

1. For each of the following, encrypt the message m using RSA with modulus $n = p \times q$ and exponent e to obtain the ciphertext c. Then find the decryption exponent d, ✓ and verify that $c^d \equiv m (\bmod n)$:

   $n = p \times q = 65$

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

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

   $\phi(n) = (5-1)(13-1) = 4 \times 12 = 48$

   $de \equiv 1 \bmod \phi(n)$

   $7d \equiv 1 \bmod 48$

   $C = 6^7 \bmod 65$ // $c^d \bmod 65 = 6$

2. Alice chooses primes $p = 113$ and $q = 167$ and encryption exponent $e = 71$. What public modulus does she publish? What is her decryption exponent?

   $71d \equiv 1 \bmod (113-1)(167-1)$

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...)

A	B	C	D	. . .	Y	Z
00	01	02	03		24	25

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

   $d \bmod 116749$ $\qquad \Phi(m) = 312 \times 372$

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

   $ed \equiv 1 \bmod \Phi(m)$ $\qquad m-1$

   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? d

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?

Exercise (Conti...)

~~8~~ Lynette has public RSA modulus $n = 119 = \underline{7 \times 17}$ and public exponent $\underline{e = 5}$. She wants to sign the document $m = 7$ //

$3^d = 5$

(7, d)) Find d

$7^d = 5$

✓ a) What is the signed document?

$= -2 \cdot 7 + 3 \cdot 40 - 15 \cdot 7$

$1 = 3 \cdot 40 - 17 \cdot 7$

b) Show that Alex calculation verifies that the document you produced in part (a) is valid.

$(7^d)^5 \bmod 119 = \underline{\underline{7}}$

$7^{-1} = -17 \bmod 40$

$= 23$

9. Lynette uses the RSA signature with public modulus $\underline{55}$ and public encryption exponent $\underline{7}$. 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?

$7^{-1} = 23$

$(3^{23})^7$

$$(3, 27), \qquad (12, 23), \qquad (9, 12), \qquad (19, 39)$$