RSA Cryptosystem

Cryptosystems

- Message → Coded message (Encryption)
- (Text) → (Ciphertext)

- Encoded message → Original message (Decryption)
- (Ciphertext) → (Plain text)

Cryptosystem – Ceaser cypher

- A →0+3=3 →D Encryption HI → 0708 → 1011→KL
- B→1+3=4 →E Decryption XDA → 23 03 00
- C→2 → F → 20 00 23
- D→3 → UAX
- E →4
- F 5
- G 6 (Shift key k=3)
- H 7
- W→22+3 = 25 →Z
- X→23+3=26 =0 →A
- Y→24+3=27 =1 →B
- Z→25+3=28 =2 → C

Shift Cyphers

- k= 5
- A→F
- B→G

- Y→D
- Z→E
- Find encrypted message of ‘ARE’.
- A→0 0+5=5 =F
- R→17 17+5=22=W
- E→4 4+5=9=J
- Encrypted msg= FWJ

RSA Cryptosystem-Introduction

- Ronald Rivest, Adi Shamir, and Leonard Adleman—introduced the RSA system in 1976.
- In the RSA cryptosystem, each individual has an encryption key (n, e) where $n = pq$, the modulus is the product of two large primes p and q, say with 200 digits each, and an exponent e that is relatively prime to
- $\varphi(n)=(p-1)(q-1)$. i.e. $\gcd(e, \varphi(n))=1$ $p=7, q=5, n=35$ $\varphi(n)=24$
- To produce a usable key, two large primes must be found. This can be done quickly on a computer using probabilistic primality tests.
- However, the product of these primes $n = pq$, with approximately 400 digits, cannot, as far as is currently known, be factored in a reasonable length of time.
- As we will see, this is an important reason why decryption cannot, as far as is currently known, be done quickly without a separate decryption key.

RSA Encryption

- To encrypt messages using a particular key (n, e), we first translate a plaintext message M into sequences of integers.
- We first translate each plain text letter into a two-digit number, using the same translation we employed for shift ciphers, with one key difference.
- That is, we include an initial zero for the letters A through J, so that A is translated into 00, B into 01, . . . , and J into 09.
- Then, we concatenate these two-digit numbers into strings of digits.
- Next, we divide this string into equally sized blocks of $2N$ digits, where $2N$ is the largest even number such that the number 2525 . . . 25 with $2N$ digits does not exceed n.
- After these steps, we have translated the plaintext message M into a sequence of integers $m_1, m_2, \ldots, m_k$ for some integer k.

RSA Encryption

- Encryption proceeds by transforming each block m_i to a ciphertext block c_i . This is done using the function

$$C = M^e \ \mathbf{mod}\ n.$$

- We leave the encrypted message as blocks of numbers and send these to the intended recipient. Because the RSA cryptosystem encrypts blocks of characters into blocks of characters, it is a block cipher.

Encryption example

Encrypt the message STOP using the RSA cryptosystem with key (2537, 13). Note that $2537 = 43 \cdot 59$, $p = 43$ and $q = 59$ are primes, and

$$\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1.$$

Solution: To encrypt, we first translate the letters in STOP into their numerical equivalents. We then group these numbers into blocks of four digits (because $2525 < 2537 < 252525$), to obtain

1819 1415.

We encrypt each block using the mapping

$$C = M^{13} \textbf{ mod } 2537.$$

Computations using fast modular multiplication show that 1819^{13} **mod** $2537 = 2081$ and 1415^{13} **mod** $2537 = 2182$. The encrypted message is 2081 2182.

n=2537=43 x 59 → p=43, q=59

Φ(n)=(p-1)(q-1)=42 x 58 = 2436

Given e=13.

Gcd(13, 2436)=1

Modular multiplication

- To find 1819^{13} (mod 2537)
- 1819^2 = 3308761 = 1304x2537 + 513
- $1819^2 = 513$ (mod 2537)
- Home work:
- Find $(1819^2)^6 = (513)^6$ (mod 2537)
- You will get $(1819)^{12}$ (mod 2537) = y, say.
- 1819^{13} (mod 2537) = 1819 y (mod 2537)

Example Encryption:

- Let p=3, q=5
- n=pq=15
- $\Phi(n)=(p-1)(q-1)=2x4=8$
- e=relatively prime to $\Phi(n) \rightarrow$ gcd(e,8)=1
- e=7
- Encrypt m=31
- C=M^e (mod n) → C= 31^7 (mod 15)
- 31= 1 (mod15)
- 31^7 = 1^7 (mod 15)
- C=1

RSA Decryption

- The plaintext message can be quickly recovered from a ciphertext message when the decryption key d, an inverse of e modulo $(p - 1)(q - 1)$, is known. [Such an inverse exists because $\gcd(e, (p - 1)(q - 1)) = 1$.] To see this, note that if $de \equiv 1 \pmod{(p - 1)(q - 1)}$, there is an integer k such that $de = 1 + k(p - 1)(q - 1)$. It follows

$$C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} \pmod{n}.$$

RSA Decryption

innovate achieve lead

$$C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 = M \pmod{p}$$

and

$$C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 = M \pmod{q}.$$

- Because gcd(p, q) = 1, it follows by the Chinese remainder theorem that

$$C^d \equiv M \pmod{pq}.$$

Example decryption

- Let p=3, q=11
- n=pq=33
- Φ(n)=(p-1)(q-1)=20
- Public key (n,e)=(33,7)
- Decipher the message C=4.

- de=1 mod phi(n) → d 7=1 (mod 20) →d=3
- Decipher key =(n,d)= (33, 3) Private key
- M= C^d (mod n) = 4^3 (mod 33) = 64 (mod 33)= 31

Decryption example

P=43, q=59

We receive the encrypted message 0981 0461. What is the decrypted message if it was encrypted using the RSA cipher from Example 8?

Solution: The message was encrypted using the RSA cryptosystem with $n = 43 \cdot 59$ and exponent 13. As Exercise 2 in Section 4.4 shows, $d = 937$ is an inverse of 13 modulo $42 \cdot 58 = 2436$. We use 937 as our decryption exponent. Consequently, to decrypt a block C, we compute

$$M = C^{937} \mathbf{mod}\ 2537.$$

To decrypt the message, we use the fast modular exponentiation algorithm to compute 0981^{937} **mod** $2537 = 0704$ and 0461^{937} **mod** $2537 = 1115$. Consequently, the numerical version of the original message is 0704 1115. Translating this back to English letters, we see that the message is HELP. ◀

d (13)=1 (mod 2436)
Gcd(2436, 13)= 1
1= r 2436 + s 13 Use extended Eulidean Algo to find r and s.
s is the decryption key→ d=s

RSA as a Public Key System

- Using RSA, it is possible to rapidly construct a public key by finding two large primes *p* and *q*, each with more than 200 digits, and to find an integer e relatively prime to $(p − 1)(q − 1)$.
- When we know the factorization of the modulus n, that is, when we know p and q, we can quickly find an inverse d of e modulo $(p − 1)(q − 1)$.
- Knowing d lets us decrypt messages sent using our key. However, no method is known to decrypt messages that is not based on finding a factorization of n, or that does not also lead to the factorization of n.
- Hence, RSA cryptosystem suitable for public key cryptography.

Cryptographic Protocols

- Key Exchange:
- Suppose that Alice and Bob want to share a common key. The protocol follows these steps, where the computations are done in $\mathbf{Z}_p$.
- (1) Alice and Bob agree to use a prime p and a primitive root a of p.
- (2) Alice chooses a secret integer k_1 and sends a^{k1} **mod** p to Bob.
- (3) Bob chooses a secret integer k_2 and sends a^{k2} **mod** p to Alice.
- (4) Alice computes $(a^{k2})^{k1}$ **mod** p.
- (5) Bob computes $(a^{k1})^{k2}$ **mod** p.
- At the end of this protocol, Alice and Bob have computed their shared

$$(a^{k_2})^{k_1} \mathbf{\ mod\ } p = (a^{k_1})^{k_2} \mathbf{\ mod\ } p.$$

DIGITAL SIGNATURES

- Suppose that Alice's RSA public key is (n, e) and her private key is d.
- Alice encrypts a plaintext message x using the encryption function $E_{(n,e)}(x) = x^e \textbf{ mod } n$.
- She decrypts a ciphertext message y using the decryption function $D_{(n,e)} = x^d \textbf{ mod } n$.
- Alice wants to send the message M so that everyone who receives the message knows that it came from her.
- Just as in RSA encryption, she translates the letters into their numerical equivalents and splits the resulting string into blocks $m_1, m_2, \ldots, m_k$ such that each block is the same size which is as large as possible so that $0 \leq m_i \leq n$ for $i = 1, 2, \ldots, k$.

DIGITAL SIGNATURES

- She then applies her *decryption function* $D_{(n,e)}$ to each block, obtaining $D_{n,e}(m_i)$, $i = 1, 2, \ldots, k$. She sends the result to all intended recipients of the message.
- When a recipient receives her message, they apply Alice's encryption function $E_{(n,e)}$ to each block, which everyone has available because Alice's key (n, e) is public information. The result is the original plaintext block because $E_{(n,e)}(D_{(n,e)}(x)) = x$.
- So, Alice can send her message to as many people as she wants and by signing it in this way, every recipient can be sure it came from Alice.

Signature example

- Suppose Alice's public RSA cryptosystem key is the same as in Example 8. That is, $n = 43 \cdot 59 = 2537$ and $e = 13$. Her decryption key is $d = 937$, as described in Example 9. She wants to send the message "MEET AT NOON" to her friends so that they are sure it came from her. What should she send?

Signature example

Solution: Alice first translates the message into blocks of digits, obtaining 1204 0419 0019 1314 1413 (as the reader should verify). She then applies her decryption transformation $D_{(2537,13)}(x) = x^{937}$ **mod** 2537 to each block. Using fast modular exponentiation (with the help of a computational aid), she finds that 1204^{937} **mod** 2537 = 817, 419^{937} **mod** 2537 = 555, 19^{937} **mod** 2537 = 1310, 1314^{937} **mod** 2537 = 2173, and 1413^{937} **mod** 2537 = 1026.

So, the message she sends, split into blocks, is 0817 0555 1310 2173 1026. When one of her friends gets this message, they apply her encryption transformation $E_{(2537,13)}$ to each block. When they do this, they obtain the blocks of digits of the original message which they translate back to English letters. ◄

p=7, q=13

- Find n=pq =91
- Phi(n)= 6 x 12= 72
- e= relatively prime to phi(n) =5

- Public key = (n,e)=(91, 5)
- Calculate private key (n,d).
- de=1 (mod phi(n))→ 5d = 1 (mod 72)
- Gcd(72,5):
- 72=5 x 14 +2
- 5 = 2 x 2 +1
- 2 = 1 x2 + 0
- gcd(72,5)=1

1=5-2x2
= 5 – 2 (72 – 5 x 14)
= 29 x 5 – 2 x 72
By extended Euclidean algo

d=29

Private key =(n, d)
=(91, 29)

Verification: de (mod n) =
29x5 (mod 72)
= 145 (mod 72) = 1 (mod 72)

THANKS