Network Security and Ciphers

Dr. G. Omprakash

Assistant Professor, ECE, KLEF

Aim of the session

To familiarize students with an understanding of fundamental concepts of security models and cryptographic algorithms and also they will learn about symmetric key ciphers and asymmetric key ciphers

Learning Outcomes

At the end of this session, you should be able to:

- Explain the classic encryption techniques
- Describe Symmetric and Asymmetric Key encryption

Overview

1. Introduction to Security
2. Symmetric-Key Ciphers
    - Substitution Cipher
        - Monoalphabetic Ciphers
        - Playfair Cipher
    - Transposition Ciphers
        - Columnar Transposition
        - Rail fence Cipher
3. Asymmetric-Key Cipher
    - RSA Cryptosystem

Introduction to Security

Introduction

- We are living in the information age
- Information is an asset that has a value like any other asset
- Information needs to be secured from attacks
  - **Confidentiality** : Information needs to be hidden from unauthorized access
  - **Integrity** : protected from unauthorized change
  - **Availability**: available to an authorized entity when it is needed
- We should me able to maintain confidentiality even when data is transmitted from one computer to another

Security Goals

- **Confidentiality** : Information needs to be hidden from unauthorized access when it is stored or transmitted
  - It is probably the most common aspect of information security
  - Eg: Data in the Bank server
- **Integrity**: refers to changes to be done only by authorized entities and through authorized mechanisms.
  - Interruption in the system, power surge can cause integrity violations
  - Eg. Changes in account balance
- **Availability**: The information created and stored by an organization needs to be available to authorized entities
  - Eg: Access to personal bank accounts

Security Attacks

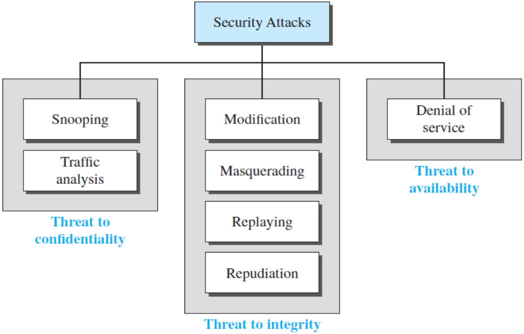


Figure: Attacks with relation to security goals

Attacks Threatening Confidentiality

- **Snooping**
  - Snooping refers to unauthorized access to or interception of data
  - A confidential file can be intercepted during transmission and its contents are used for benefits
  - Prevention: Data can be made nonintelligible to the intercepter by using encipherment techniques
- **Traffic Analysis**
  - Although the data is made nonintelligible for the intercepter, they can obtain some other types of information by monitoring online traffic
  - See the e-mail address of sender and receiver to guess the nature of the transaction

Attacks Threatening Integrity

- **Modification**: After intercepting or accessing information, the attacker modifies the information to benefit themselves
  - Eg: Customer sends a message to a bank to initiate some transaction. The attacker intercepts the message and changes the type of transaction to their own benefit.
- **Masquerading/Spoofing** happens when the attacker impersonates somebody else
  - An attacker might steal the bank card and PIN of a bank customer and pretend to be the customer!!

Attacks Threatening Integrity

- **Replaying**: The attacker obtains a copy of a message sent by a user and later tries to replay it.
- **Repudiation**: It is performed by one of the two parties in the communication: Sender/Receiver
  - The sender of the message might later deny that she has sent the message
  - The receiver of the message might later deny that he has received the message.

Attacks Threatening Availability

- **Denial of Service**: may slow down or totally interrupt the service of a system. Strategies are:
  - Attacker can send so many bogus requests to a server that the server crashes because of the heavy load.
  - Attacker can intercept and delete a server's response to a client.
  - Attacker may also intercept requests from the clients, causing the clients to send requests many times and overload the system.

Cryptography

- Cryptography comes from the Greek words for ”*secret writing*”.
- **Cipher** is a character-for-character or bit-for-bit transformation
  - No regard to the linguistic structure of the message
- **Code** replaces one word with another word or symbol.
- **Confidentiality (security goal) can be achieved using ciphers.**

Classification of Cipher

Ciphers

- Symmetric-Key Ciphers
  - Substitution Ciphers
    - Monoalphabetic Ciphers (Additive/Caesar)
    - Playfair Ciphers
  - Transposition Ciphers:
    - Columnar Transposition
    - Rail Fence Cipher
  - Data Encryption Standard (DES)
- Asymmetric-Key Ciphers
  - RSA Algorithm (Rivest, Shamir, and Adleman).

Symmetric-Key Ciphers

Symmetric-Key Ciphers

- A **symmetric-key** cipher uses the same key for both encryption and decryption
  - Key can be used for bidirectional communication
- Encryption of the plaintext P using key K gives the ciphertext C

$$C = E_K(P)$$

- $P = D_K(C)$ represents the decryption of C to get the plaintext again.

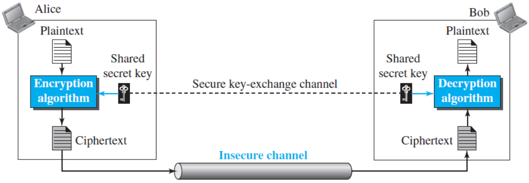


Figure: General idea of a symmetric-key cipher

Merits and Demerit of Symmetric-Key Cipher

- **Merits**
  - It is fast and convenient to set up.
  - Method is simple and easy to understand and master
- **De-Merit**
  - The key must be known by both sender and recipient

Substitution Cipher: Monoalphabetic Ciphers

- Traditional symmetric-key Ciphers are classified as
  - **Substitution ciphers**
    - Monoalphabetic Ciphers
  - **Transposition ciphers**

Substitution ciphers

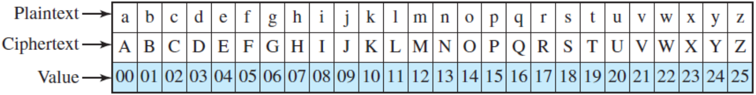
- A substitution cipher replaces one symbol with another
- In a substitution cipher, each letter (group) of letter(s) is replaced by another letter(s) to disguise it.
- **Monoalphabetic Ciphers**: In a monoalphabetic cipher, a character (or a symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext regardless of its position in the text

Substitution Cipher: Monoalphabetic Ciphers

- Simplest monoalphabetic cipher is the **additive cipher** (or **shift cipher**).
- Julius Caesar used an additive cipher, with a key of 3, to communicate with his officers.
- For this reason, additive ciphers are sometimes referred to as the *Caesar cipher*.
- **Caesar cipher**: $a \implies D$, $b \implies E$,...,$z \implies C$
  - $attack \implies DWWDFN$
- **Generalization of the Caesar cipher**: Alphabet to be shifted by k letters, instead of three

Additive Cipher

Use the additive cipher with key = 15 to encrypt the message “hello”.



Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

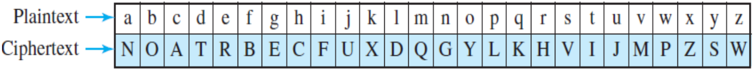
Plaintext	Adding Key (15)	mod 26	Ciphertext
h $\Longrightarrow$ 7	22	22	22 $\Longrightarrow$ W
e $\Longrightarrow$ 4	19	19	19 $\Longrightarrow$ T
l $\Longrightarrow$ 11	26	0	0 $\Longrightarrow$ A
l $\Longrightarrow$ 11	26	0	0 $\Longrightarrow$ A
o $\Longrightarrow$ 14	29	3	3 $\Longrightarrow$ D

Ciphertext: WTAAD

Analyse and apply Caesar cipher to encrypt and decrypt the message ”NETWORKS,” and the key(shift) value is 4.

Drawback of Additive Cipher

- Additive ciphers are vulnerable to attacks using exhaustive key searches (brute force attacks).
- The key domain of the additive cipher is very small (26)
  - Easily launch a brute-force attack on the ciphertext.
- **Better solution**: Create a mapping between each plaintext character and the corresponding ciphertext character



Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	N	O	A	T	R	B	E	C	F	U	X	D	Q	G	Y	L	K	H	V	I	J	M	P	Z	S	W

Playfair Cipher

Playfair cipher is a symmetric encryption technique that encrypts letters in pairs (digraphs) using a 5x5 grid

- The keyword is written into a 5x5 grid, with the remaining letters of the alphabet (excluding ”I” and ”J”, which are treated as the same) filling the empty squares **in alphabetical order**.
- Keyword: ”MONARCHY”; Plaintext: ”INSTRUMENTS”

Playfair Cipher

Keyword: "MONARCHY"; Plaintext: "INSTRUMENTS"

Key Matrix:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

Preprocess the Plaintext

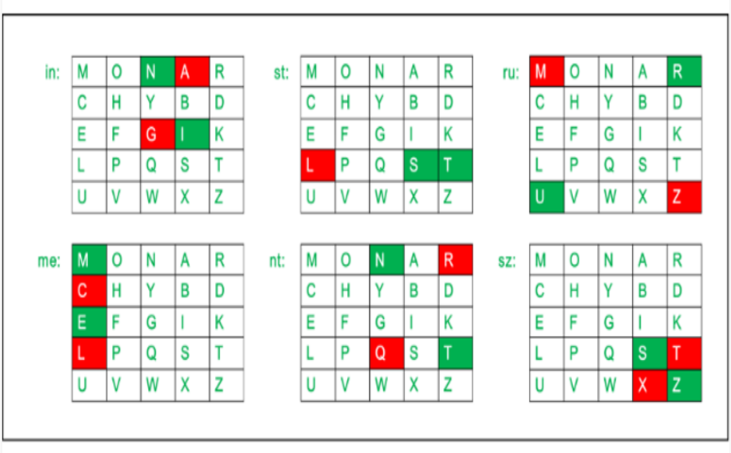
- Break the message into digraphs (pairs of two letters).
- If both letters in a digraph are the same (e.g., "EE"), insert an "Z" between them.
- If there's an odd number of letters, add an "Z" at the end.
- After Split: 'IN' 'ST' 'RU' 'ME' 'NT' 'SZ'

Playfair Cipher: Encryption

For each pair:

- **Same row**: Replace each letter with the letter to its right (wrap around).
- **Same column**: Replace each letter with the letter below it (wrap around)
- **Rectangle**: Replace with letters on the same row but at the opposite corners.

Playfair Cipher: Example



in:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

st:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

ru:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

me:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

nt:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

sz:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

Playfair Cipher: Example 1

- digraph: IN
  - Rectangle rule: Form a rectangle and replace letter with same row letter
  - Rectangle rule: I ⟹ G; N ⟹ A
- digraph: ST
  - Same row: (letter to the right) S ⟹ T; T ⟹ L
- digraph: RU
  - Rectangle rule: R ⟹ M; U ⟹ Z
- digraph: ME
  - Same Column: M ⟹ C; E ⟹ L
- digraph: NT
  - Rectangle rule: N ⟹ R; T ⟹ Q
- digraph: SZ
  - Rectangle rule: S ⟹ T; Z ⟹ X

Ciphertext: **GATLMZCLRQTX**

Playfair: Example 2

Keyword: "GUIDANCE"; Plaintext: "SEMESTEREXAM"

Key Matrix:

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

Preprocess the Plaintext

- Break the message into digraphs (pairs of two letters).
- 'SE' 'ME' 'ST' 'ER' 'EX' 'AM'

Example 2

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

Example 2

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph:SE $\Longrightarrow$ RB

Example 2

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph:SE $\Longrightarrow$ RB

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

Example 2

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph:SE $\Longrightarrow$ RB

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph: ME $\Longrightarrow$ LB

Example 2

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph:SE $\Longrightarrow$ RB

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph: ME $\Longrightarrow$ LB

Example 2

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph:SE $\Longrightarrow$ RB

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph: ST $\Longrightarrow$ TP

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph: ME $\Longrightarrow$ LB

Example 2

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph:SE $\Longrightarrow$ RB

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph: ST $\Longrightarrow$ TP

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph: ME $\Longrightarrow$ LB

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

Example 2

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph:SE $\Longrightarrow$ RB

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph: ST $\Longrightarrow$ TP

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph: ME $\Longrightarrow$ LB

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph: ER $\Longrightarrow$ LX

Example 2

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

Example 2

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph:EX $\Longrightarrow$ LI

Example 2

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph:EX $\Longrightarrow$ LI

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

Example 2

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph:EX $\Longrightarrow$ LI

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph: AM $\Longrightarrow$ DO

Example 2

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph:EX ⟹ LI

G	U	I	D	A
N	C	E	B	F
H	K	L	M	O
P	Q	R	S	T
V	W	X	Y	Z

digraph: AM ⟹ DO

Ciphertext: ”RBLBTPLXLIDO”

Example: 3

Plaintext: 'HELLO'; Key: 'GUIDANCE'
'LL' is duplicate $\Longrightarrow$ becomes LX, LO
digraphs: 'HE' 'LX' 'LO'
Ciphrtext:'LNRIMH'

Transposition Ciphers

A transposition cipher reorders symbols.

Types:

- Columnar Transposition

Columnar Transposition Technique

Steps to obtain cipher text

- In a rectangle of pre-defined size, write the plain-text message row by row.
- Use the key to get the column reordering
  - column key="VEGA" $\Longrightarrow$ 4231
- Rearrange the columns and write the text column wise
- Cipher-text is obtained!!

Columnar Transposition: Encryption Example

Original message: "INCLUDEHELPISAWESOME".

C1	C2	C3	C4
I	N	C	L
U	D	E	H
E	L	P	I
S	A	W	E
S	O	M	E

4	2	3	1
L	N	C	I
H	D	E	U
I	L	P	E
E	A	W	S
E	O	M	S

- column key="VEGA"
- Alphabetical order in the given key "VEGA" $\Longrightarrow$ 4231
- **Plaintext is written horizontally, in rows**
- Reorder the columns
- Ciphertext is read out by columns: LHIEENDLAOCEPWMIUESS

Columnar Transposition: Decryption

Given: LHIEENDLAOCEPWMIUESS; column key = "VEGA" $\implies$ 4231

Write the text in 4 columns

(column-wise)

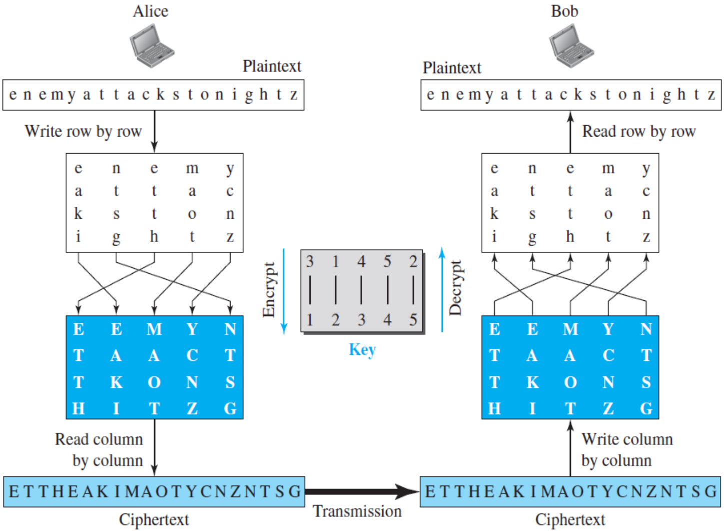
4	2	3	1
L	N	C	I
H	D	E	U
I	L	P	E
E	A	W	S
E	O	M	S

Reorder the columns as per key

1	2	3	4
I	N	C	L
U	D	E	H
E	L	P	I
S	A	W	E
S	O	M	E

Read the text row-wise: "INCLUDEHELPISAWESOME"

Columnar Transposition: Example



Alice

Plaintext

e n e m y a t t a c k s t o n i g h t z

Write row by row

e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	z

Encrypt

3	1	4	5	2
1	2	3	4	5

Key

Decrypt

E	E	M	Y	N
T	A	A	C	T
T	K	O	N	S
H	I	T	Z	G

Read column by column

ETTHEAKIMAOTYCNZNTSG

Ciphertext

Transmission

Bob

Plaintext

e n e m y a t t a c k s t o n i g h t z

Read row by row

e	n	e	m	y
a	t	t	a	c
k	s	t	o	n
i	g	h	t	z

E	E	M	Y	N
T	A	A	C	T
T	K	O	N	S
H	I	T	Z	G

Write column by column

ETTHEAKIMAOTYCNZNTSG

Ciphertext

Rail Fence Cipher

- **Rail Fence Cipher**: Encryption
  - **Step 1**: The plain text is written as a sequence of diagonals.
  - **Step 2**: To obtain the cipher text, the text is read as a sequence of rows
- Example : “INCLUDEHELPISAWESOME”. Key=2
- No of columns=length of the text=20; No Of Rows=2 (Key)

I		C		U		E		E		P		S		W		S		M	
	N		L		D		H		L		I		A		E		O		E

- Write the message in a zigzag manner then read it out direct row-wise to change it to cipher-text
- Cipher-text: ICUEEPSWSMNLDHLIAEOE
- Rail-Fence Technique is very easy to break by any cryptanalyst.

Rail Fence Cipher: Encryption

Examples: `https://www.geeksforgeeks.org/rail-fence-cipher-encryption-decryption/`

- Input : "attack at once"; Key=2;
- No of columns=length of the text=14; No Of Rows=2 (Key)

a		t		c		-		t		o		c	
	t		a		k		a		-		n		e

- Output : atc toctaka ne

- Input : "defend the east wall"; Key=3;
- No of columns=length of the text=20; No Of Rows=3

d				n				h				a				w			
	e		e		d		t		e		e		s		-		a		l
		f				-				-				t				l	

- Output : dnhaweedtees alf tl

Rail Fence Cipher: Decryption

- Input : ”atc toctaka ne” ; Key=2;
- No Of Columns=14; Rows=2; write ”*” in a zigzag manner

*		*		*		*		*		*		*	
	*		*		*		*		*		*		*

- Replace ”*” with the characters of the cipher text

Rail Fence Cipher: Decryption

- Input : "atc toctaka ne" ; Key=2;
- No Of Columns=14; Rows=2; write "*" in a zigzag manner

*		*		*		*		*		*		*	
	*		*		*		*		*		*		*

- Replace "*" with the characters of the cipher text

a		t		c		-		t		o		c	
	t		a		k		a		-		n		e

- Output : "attack at once"

Asymmetric-Key Cipher

Asymmetric-Key Cryptography

- **Asymmetric-key** cryptography uses uses two keys: one private and one public
  - Also called public key cryptography
- For n users:
  - $\frac{n(n-1)}{2}$ secrets are required for symmetric-key cryptography
  - Only n personal secrets are needed in asymmetric-key cryptography
- It requires keys of at least 2048 bits for good security (versus 256 bits for symmetric- key algorithms)
  - Hence it is quite slow
- Asymmetric-key cryptography is normally used to encrypt or decrypt small pieces of information

Asymmetric-key cryptosystem

- Asymmetric key cryptography uses two separate keys: one private and one public.
- **Encryption** $\Longrightarrow$ using **Public Key**
- **Decryption** $\Longrightarrow$ using **Private key**

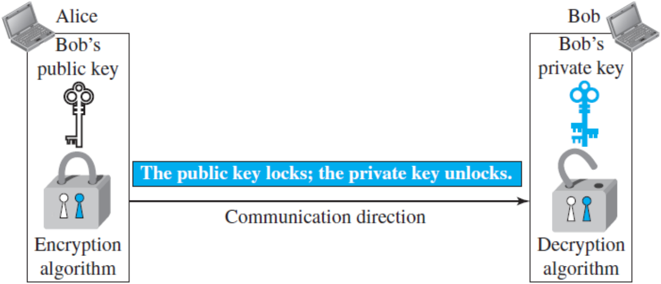


Figure: Credits: Forouzan. Locking and unlocking in asymmetric-key cryptosystem

Symmetric-key vs Asymmetric-key ciphers

Symmetric-key Cipher	**Asymmetric-key Cipher**
Symmetric-key cryptography is based on sharing secrecy	Asymmetric-key cryptography is based on personal secrecy
For n people, $n(n-1)/2$ shared secrets are needed	For n people, only n personal secrets are needed
Symmetric-key cryptography is based on substitution and permutation of symbols (characters or bits)	Asymmetric-key cryptography is based on applying mathematical functions to numbers
The plaintext and ciphertext are thought of as a combination of symbols.	The plaintext and ciphertext are numbers
Encryption and decryption permute these symbols or substitute one symbol for another	Encryption and decryption are mathematical functions that are applied to numbers to create other numbers

Encryption and Decryption

- RSA is named after its inventors Rivest, Shamir, and Adleman.
- Choose two very large prime numbers p and q
  - Prime number is one that can be divided only by 1 and itself
- Find $n = p \times q$
- Find $\phi(n) = (p-1) \times (q-1)$
- Choose e such that $1 < e < \phi(n)$ and $gcd(e, \phi(n)) = 1$
- Find d such that $(e \times d)$ mod $\phi(n)$= 1 .
- Public key (e, n); Private key (d, n)
- Encrypt: $C = (P^e) mod\ n$
- Decrypt: $P = (C^d) mod\ n$
- P **is always in the form of numbers**
  - If text is given, use ASCII values of each character

Example 1

The RSA algorithm uses two prime numbers, say p=3 and q=11. Discover the possible values of Public Key(e, n), and Private Key (d, n). Encrypt the message P=4;

Example 1: Finding Keys

- Let us choose $p = 3$; $q = 11$;
- $n = 3 \times 11 = 33$
- $\phi(n) = (p-1) \times (q-1) = 2 \times 10 = 20$
- Choose $e = 3$; gcd(3,20)=1;
- Find d such that $(3 \times d)$ mod 20=1 $\implies d = 7$
- Public Key: $(e = 3, n = 33)$
- Private Key: $(d = 7, n = 33)$

Example 1: Encryption and Decryption

- Public Key: $(e = 3, n = 33)$
- Private Key: $(d = 7, n = 33)$
- Message P=4
- Encrypt: C=$(P^e)mod\ n$=$(4^3)mod$ 33=64 mod 33=31
- Decrypt: P=$(C^d)mod\ n$=$(31^7)mod$ 33=4

Example 2: Finding Keys

- Let us choose $p = 7$; $q = 11$;
- $n = 7 \times 11 = 77$
- $\phi(n) = (p - 1) \times (q - 1) = 6 \times 10 = 60$
- Choose $e = 13$; gcd(13,60)=1;
- Find d s.t $13 \times d \ mod \ 60{=}1 \implies d = 37$
- Public Key: $(e = 13, n = 77)$
- Private Key: $(d = 37, n = 77)$

Example 2: Encryption and Decryption

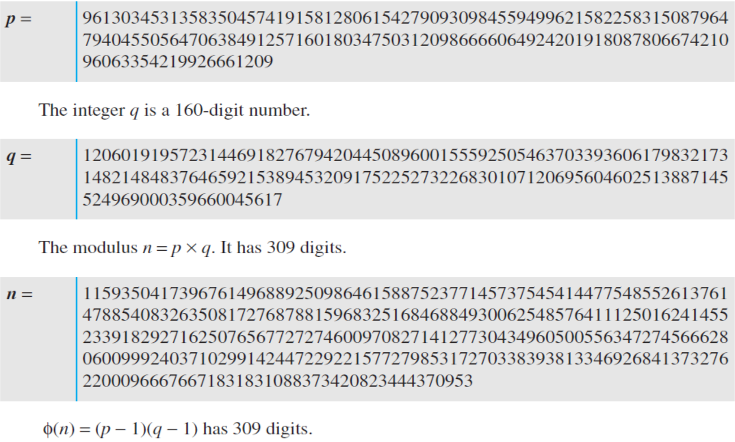
- Public Key: $(e = 13, n = 77)$
- Private Key: $(d = 37, n = 77)$
- Message P=5
- Encrypt: C=$(P^{e})mod\ n$=$(5^{13})mod\ 77$=26 mod 77=26
- Decrypt: P=$(C^{d})mod\ n$=$(26^{37})mod\ 77$=5

Finding Keys: Example 3

- Let us choose $p = 17$; $q = 11$;
- $n = 17 \times 11 = 187$
- $\phi(n) = (p-1) \times (q-1) = 16 \times 10 = 160$
- Choose $e = 7$
- Find d s.t $7 \times d \; mod \; 160{=}1 \implies d = 23$
- Public Key: $(e = 7, n = 187)$
- Private Key: $(d = 23, n = 187)$
- Find the plain text from the Ciphertext=65

RSA Realistic Numbers!!

Length of the key should be 2048-bit for good security!!



$p =$ 96130345313583504574191581280615427909309845594996215822583150879647940455056470638491257160180347503120986666064924201918087806674210 96063354219926661209

The integer q is a 160-digit number.

$q =$ 12060191957231446918276794204450896001555925054637033936061798321731482148483764659215389453209175225273226830107120695604602513887145 524969000359660045617

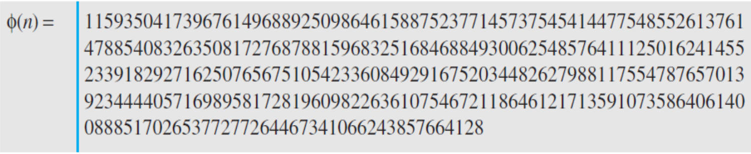
The modulus $n = p \times q$. It has 309 digits.

$n =$ 11593504173967614968892509864615887523771457375454144775485526137614788540832635081727687881596832516846884930062548576411125016241455233918292716250765677272746009708271412773043496050055634727456662806009992403710299142447229221577279853172703383938133469268413732762200096667667183183108837342082344437095 3

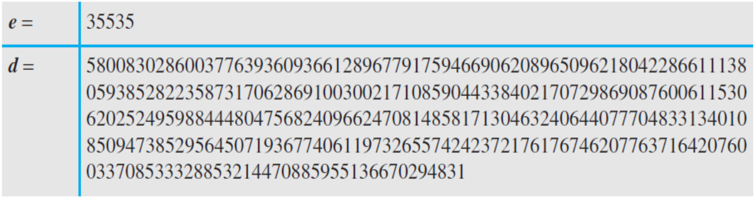
$\phi(n) = (p - 1)(q - 1)$ has 309 digits.

RSA Realistic Numbers!!

choose $e = 35535$ (the ideal is 65537). Then find d!!.



$\phi(n) =$	1159350417396761496889250986461588752377145737545414477548552613761
	4788540832635081727687881596832516846884930062548576411125016241455
	2339182927162507656751054233608492916752034482627988117554787657013
	9234440571698958172819609822636107546721186461217135910735864061400
	888517026537727726446734106624385766412 8



$e =$	35535
$d =$	5800830286003776393609366128967791759466906208965096218042286611138 0593852822358731706286910030021710859044338402170729869087600611530 6202524959884448047568240966247081485817130463240644077704833134010 8509473852956450719367740611973265574242372176176746207763716420760 033708533328853214470885955136670294831

Acknowledge various sources for the images.

Thankyou