SLIIT

Discover Your Future

IE2022 – Introduction to Cyber Security

Lecture - 05

Cryptography I

Mr. Amila Senarathne

Cryptography I

- Reading Assignment
  - CCNA Security Curriculum, Chapter 7: Cryptographic Systems

- Supplementary text
  - W. Stallings and L. Brown, “Computer Security, Principles and Practice, 2nd edition, Pearson, 2012, Chapter 2 :Cryptographic Tools.

Topics to be discussed

- Cryptographic Services
- History of cryptography
- Substitution and Transposition Ciphers
- Introduction to Symmetric and Asymmetric Encryption Algorithms
- One-time pad
- Cryptanalysis
- Cryptology

Cryptographic Services

Authentication, Integrity, and Confidentiality Cont.

- Secure communications necessitates three primary objectives:
- **Authentication** - Guarantees that the message is not a forgery and does actually come from whom it states.
- **Integrity** - Guarantees that no one intercepted the message and altered it; similar to a checksum function in a frame.
- **Confidentiality** - Guarantees that if the message is captured, it cannot be deciphered.

Authentication

Integrity

Confidentiality

Authentication

- Authentication guarantees that the message:
  - Is not a forgery.
  - Does actually come from who it states it comes from.
- Authentication is similar to a secure PIN for banking at an ATM.
  - The PIN should only be known to the user and the financial institution.
  - The PIN is a shared secret that helps protect against forgeries.

Entering an ATM Authentication PIN

Authentication Cont.

- Data nonrepudiation is a similar service that allows the sender of a message to be uniquely identified.
- This means that a sender/device cannot deny having been the source of that message. It cannot repudiate, or refute, the validity of a message sent.

Data Integrity

- Data integrity ensures that messages are not altered in transit. The receiver can verify that the received message is identical to the sent message and that no manipulation occurred.
- European nobility ensured the data integrity by creating a wax seal to close an envelope.
  - The seal was often created using a signet ring.
  - An unbroken seal on an envelope guaranteed the integrity of its contents.
  - It also guaranteed authenticity based on the unique signet ring impression.

An Unbroken Wax Seal Ensures Integrity

Data Confidentiality Cont.

- Data confidentiality ensures privacy so that only the receiver can read the message.
- Encryption is the process of scrambling data so that it cannot be read by unauthorized parties.
  - Readable data is called plaintext, or cleartext.
  - Encrypted data is called ciphertext.
  - A key is required to encrypt and decrypt a message. The key is the link between the plaintext and ciphertext.

Creating Ciphertext

- Authentication, integrity, and confidentiality are components of cryptography.
- Cryptography is both the practice and the study of hiding information.
- It has been used for centuries to protect secret documents. Today, modern day cryptographic methods are used in multiple ways to ensure secure communications.

Authentication

Integrity

Confidentiality

Creating Ciphertext Cont.

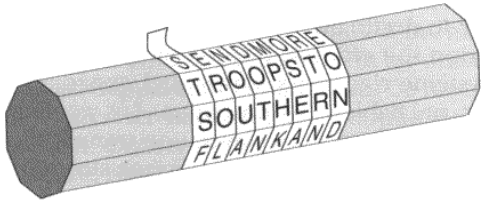
- Encryption methods uses a specific algorithm, called a cipher, to encrypt and decrypt messages.
- A cipher is a series of well-defined steps that can be followed as a procedure when encrypting and decrypting messages.
- There are several methods of creating cipher text:
  - Transposition
  - Substitution
  - One-time pad

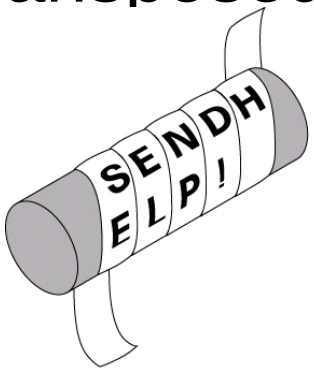
Creating Ciphertext Cont.

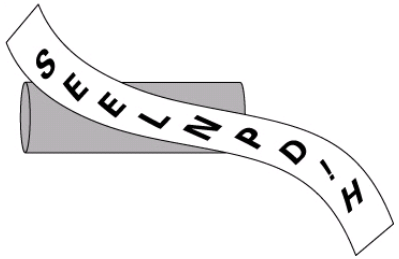
- Cryptography is both the practice and the study of hiding information.
- Cryptography is used to ensure the protection of data when that data might be exposed to untrusted parties.
- Cryptographic services are the foundation for many security implementations
- Over the centuries, various cipher methods, physical devices, and aids have been used to encrypt and decrypt text:
  - Scytale
  - Caesar cipher
  - Vigenère Cipher
  - Jefferson's encryption device
  - German Enigma machine

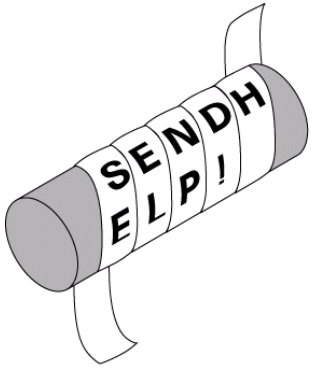
Creating Ciphertext Cont.

- Scytale
  - Earliest cryptography method was used by the Spartans in ancient Greece.
  - It is a rod used as an aid for a transposition cipher. The sender and receiver had identical rods (scytale) on which to wrap a transposed messaged.









Creating Ciphertext Cont.

- Caesar Cipher
- When Julius Caesar sent messages to his generals, he did not trust his messengers.
- Caesar encrypted his messages by replacing every letter:
  - A with a D
  - B with an E
  - and so on
- His generals knew the “shift by 3” rule and could decipher his messages.

Vigenère Cipher

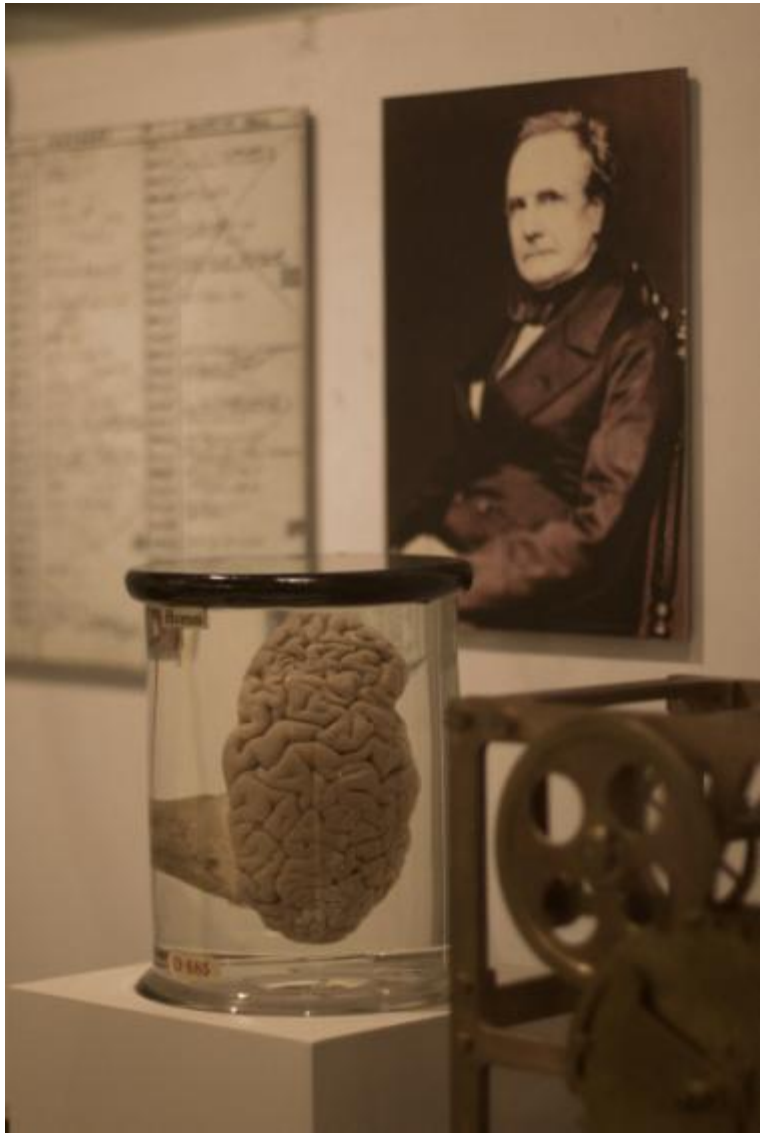
- Vigenère Cipher
- In 1586, Frenchman Blaise de Vigenère described a polyalphabetic system of encryption. It became known as the Vigenère Cipher.
- Based on the Caesar cipher, it encrypted plaintext using a multi-letter key. It is also referred to as an autokey cipher.

Vigenère Cipher Cont.

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

Note of Interest ...

- It took 300 years for the Vigenère Cipher to be broken by Englishman Charles Babbage who is known as the father of modern computers.
- Babbage created the first mechanical computer called the difference engine to calculate numerical tables.
- He then designed a more complex version called the analytical engine that could use punch cards.
- He also invented the pilot (cow-catcher).

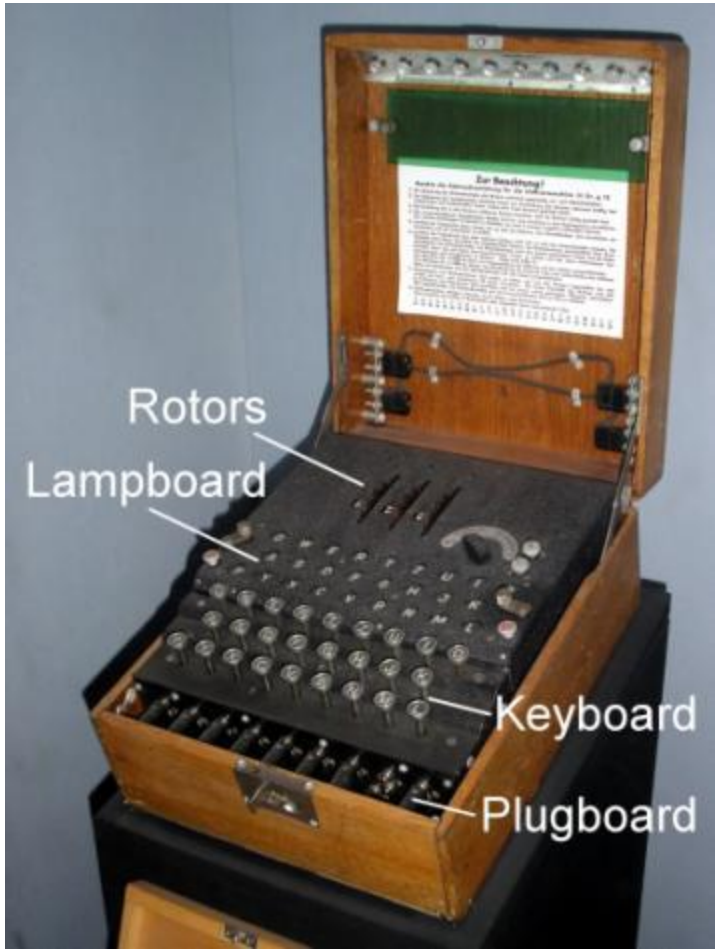


Creating Ciphertext Cont.

- Jefferson's Encryption Device
  - Thomas Jefferson, the third president of the United States, invented an encryption system that was believed to have been used when he served as secretary of state from 1790 to 1793.

Creating Ciphertext Cont.

- German Enigma Machine
  - Arthur Scherbius invented the Enigma in 1918 and sold it to Germany. It served as a template for the machines that all the major participants in World War II used.
  - It was estimated that if 1,000 cryptanalysts tested four keys per minute, all day, everyday, it would take 1.8 billion years to try them all.
  - Germany knew their ciphered messages could be intercepted by the allies, but never thought they could be deciphered.



http://users.telenet.be/d.rijmenants/en/enigma.htm

Code Talkers

- During World War II, Japan deciphered every code that the Americans created. A more elaborate coding system was needed. The answer came in the form of the Navajo code talkers.
- Code talkers were bilingual Navajo speakers specially recruited by the Marines during World War II.
- Other Native American code talkers were Cherokee, Choctaw, and Comanche soldiers.
- Not only were there no words in the Navajo language for military terms, the language was unwritten and less than 30 people outside of the Navajo reservations could speak it, and not one of them was Japanese. By the end of the war, more than 400 Navajo Indians were working as code talkers.

Transposition Ciphers

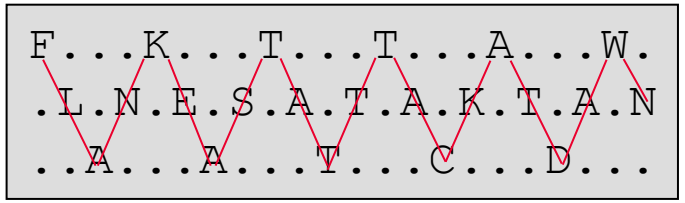
- In transposition ciphers, no letters are replaced; they are simply rearranged.
- For example: Spell it backwards.
- Modern encryption algorithms, such as the Data Encryption Standard (DES) and 3DES, still use transposition as part of the algorithm.

Transposition Ciphers - Rail Fence Cipher

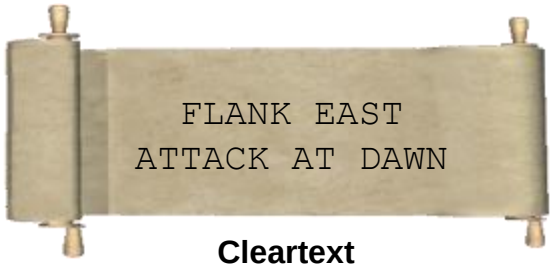
1. Solve the ciphertext.

Ciphered text

2. Use a rail fence cipher and a key of 3.



3. The cleartext message.



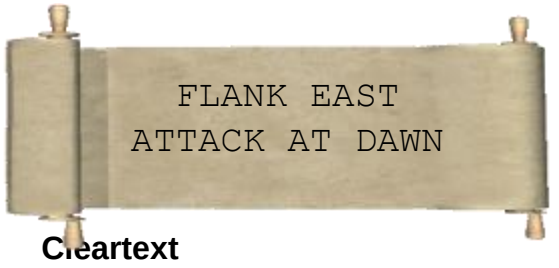
Cleartext

Substitution Ciphers

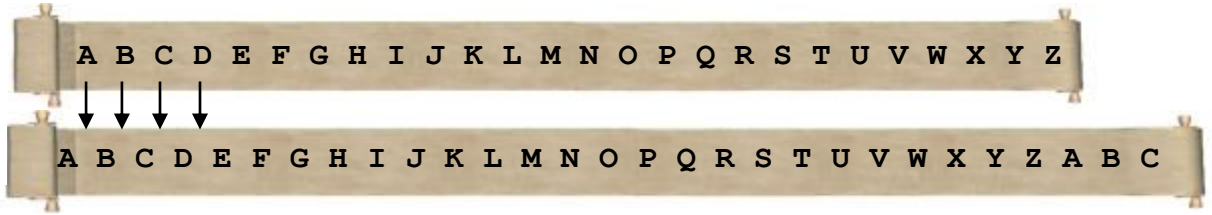
- Substitution ciphers substitute one letter for another. In their simplest form, substitution ciphers retain the letter frequency of the original message.
- Examples include:
  - Caesar Cipher
  - Vigenère Cipher

Substitution Ciphers - Encoding using the Caesar Cipher

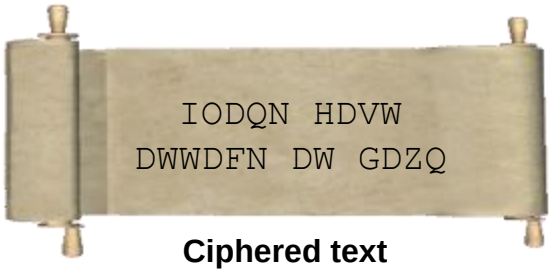
1. The cleartext message.



2. Encode using a key of 3. Therefore, A becomes a D, B an E, …

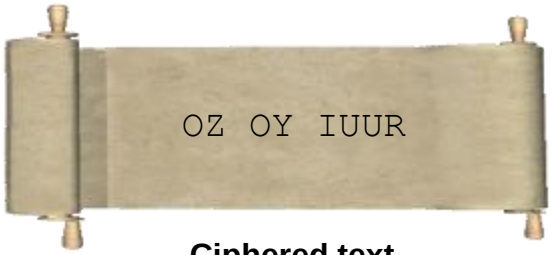


3. The encrypted message becomes …



Decoding

1. Solve the ciphertext.



Ciphered text

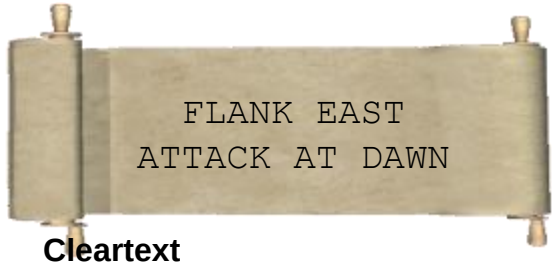
2. Use a shift of 6 (ROT6).

3. The clear text message.

Cleartext

Substitution Ciphers - Caesar Cipher Disk

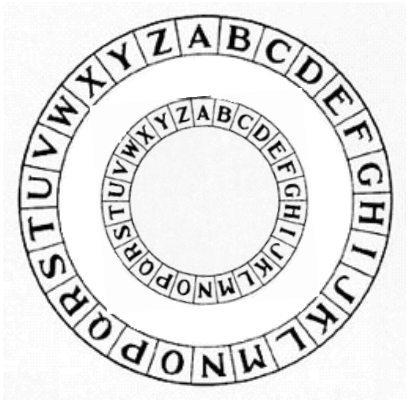
1

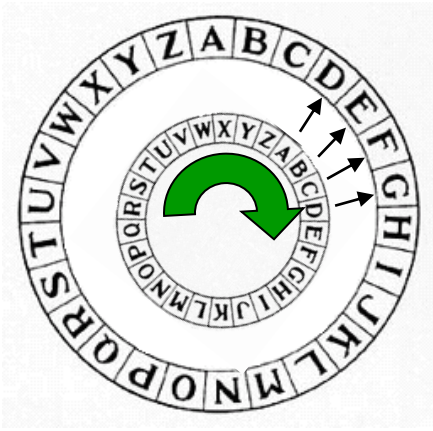


Cleartext

The cleartext message would be encoded using a key of 3.

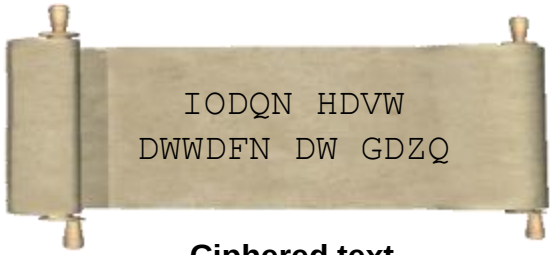
2





Shifting the inner wheel by 3, the A becomes D, B becomes E, and so on.

3



Ciphered text

The cleartext message appears as follows using a key of 3.

Substitution Ciphers - Vigenère Cipher

- The Vigenère cipher is based on the Caesar cipher, except that it encrypts text by using a different polyalphabetic key shift for every plaintext letter.
  - The different key shift is identified using a shared key between sender and receiver.
  - The plaintext message can be encrypted and decrypted using the Vigenère Cipher Table.
- For example:
  - A sender and receiver have a shared secret key: SECRETKEY.
  - The sender then uses the key to encode: FLANK EAST ATTACK AT DAWN.

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

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

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

To Decrypt ….

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

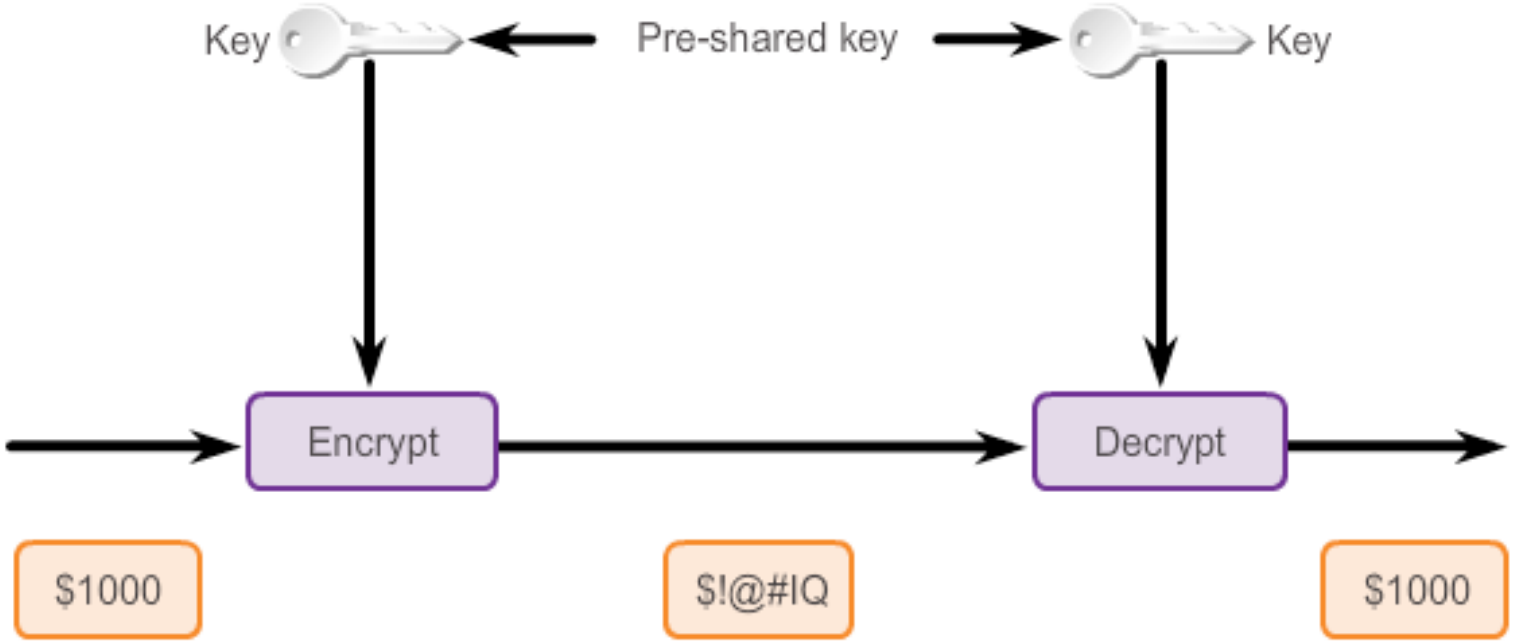
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t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

Decrypt the following ….

T	C	P	I	P	T	C	P	I	P	T	C	P	I	P	T	C	P	I	P	T
V	E	C	I	H	X	E	J	Z	X	M	A									
C	C	N	A	S	E	C	U	R	I	T	Y									

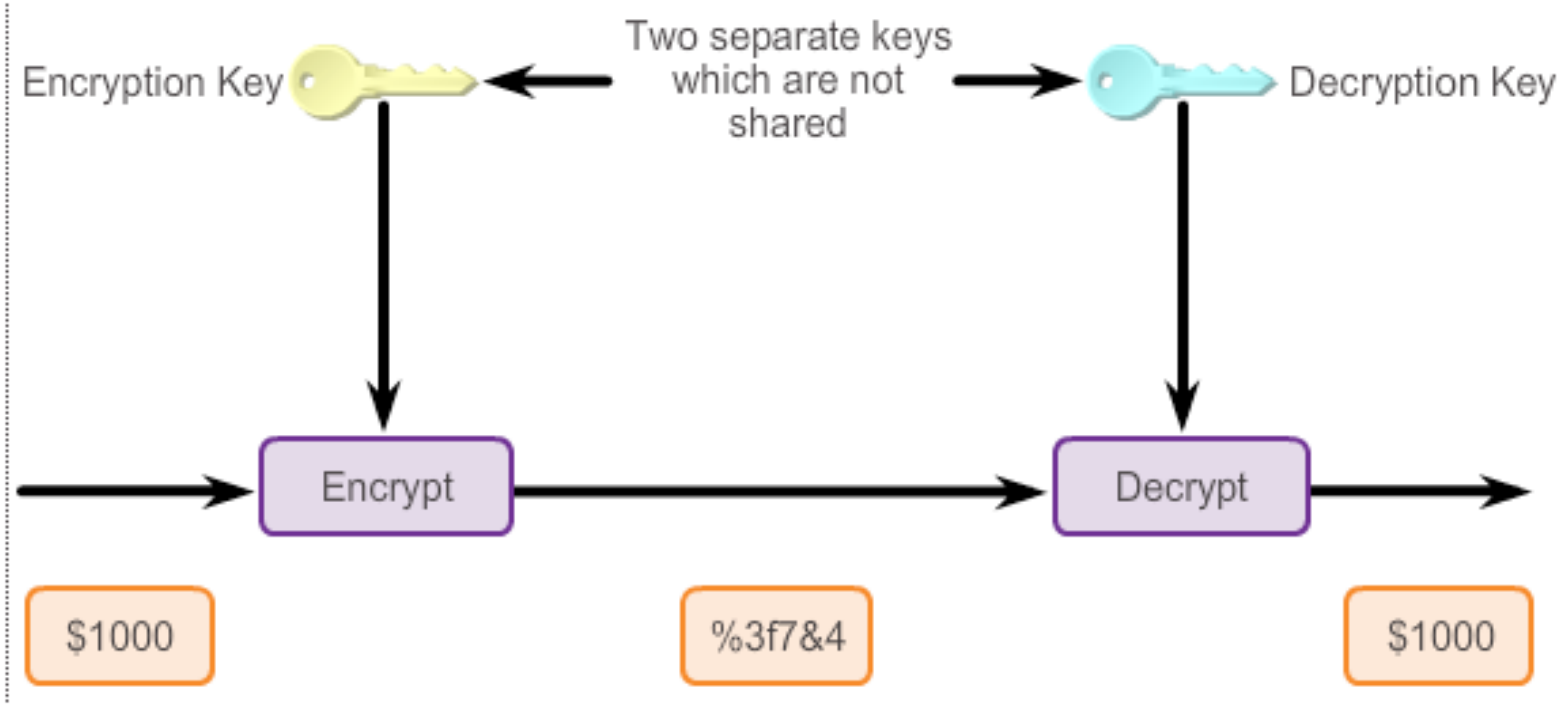
Symmetric Encryption Algorithms

- Symmetric encryption algorithms characteristics include:
  - Symmetric encryption algorithms are best known as shared-secret key algorithms.
  - A sender and receiver must share a secret key.



Asymmetric Encryption Algorithms Cont.

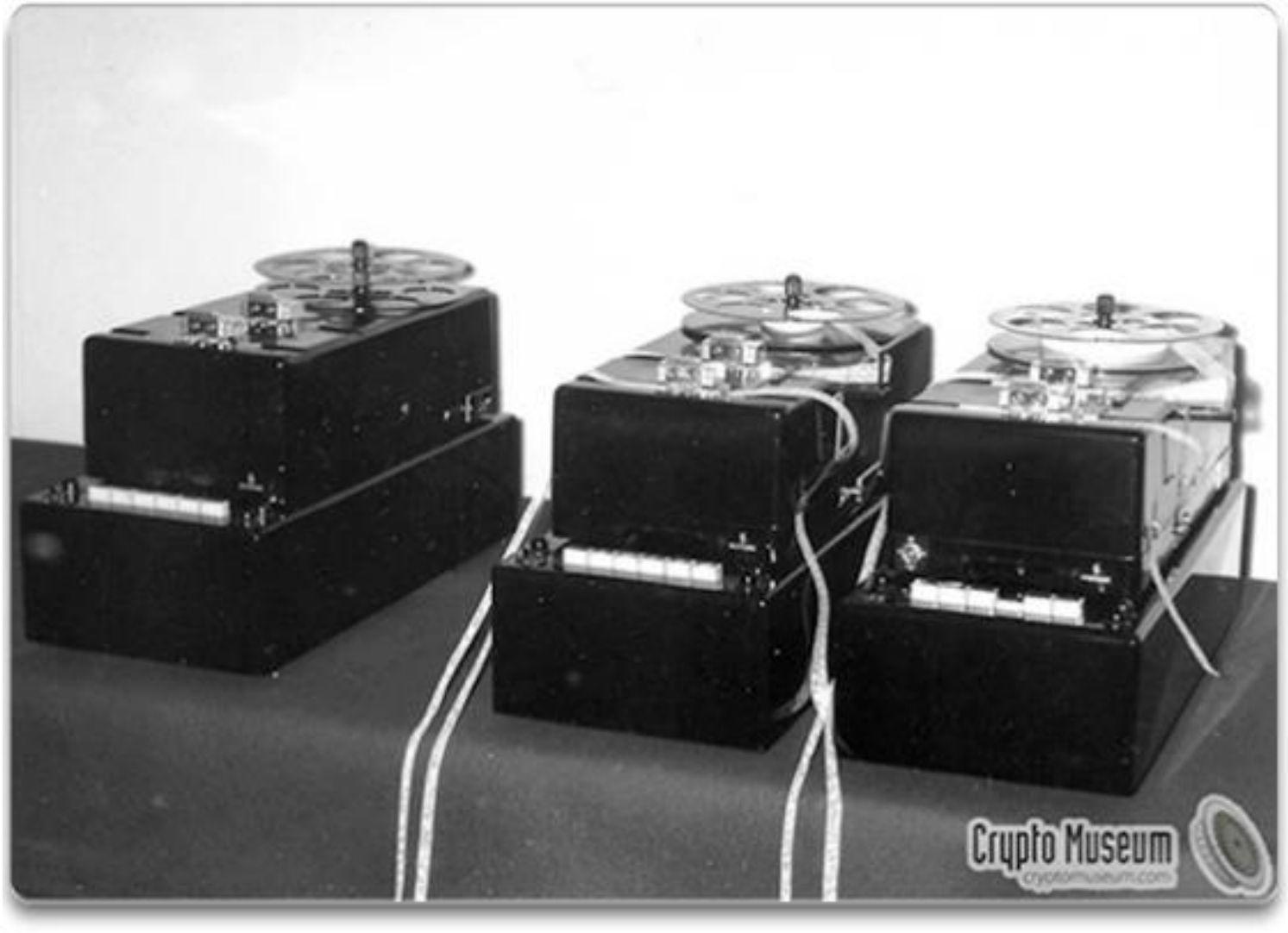
- Asymmetric encryption algorithms characteristics include:
  - Asymmetric encryption algorithms are best known as public key algorithms.
  - A sender and receiver do not share a secret key.



One-Time Pad Ciphers

- In 1917, Gilbert Vernam, an AT&T Bell Labs engineer, invented and patented the stream cipher and later co-invented the one-time pad cipher.
  - Vernam proposed a teletype cipher in which a prepared key consisting of an arbitrarily long, non-repeating sequence of numbers was kept on paper tape.
  - It was then combined character by character with the plaintext message to produce the ciphertext.
  - To decipher the ciphertext, the same paper tape key was again combined character by character, producing the plaintext.
- Each tape was used only once,; hence the name one-time pad. As long as the key tape does not repeat or is not reused, this type of cipher is immune to cryptanalytic attack, because the available ciphertext does not display the pattern of the key.

One-Time Pad Ciphers



One-Time Pad Ciphers Cont.

- Several difficulties are inherent in using one-time pads in the real world.
  - Key distribution is challenging.
  - Creating random data is challenging and if a key is used more than once, it becomes easier to break.
- Computers, because they have a mathematical foundation, are incapable of creating true random data.
- RC4 is a one-time pad cipher that is widely used on the Internet. However, because the key is generated by a computer, it is not truly random.

Cracking Code

Cryptanalysis

- The practice and study of determining the meaning of encrypted information (cracking the code), without access key/s.
- Been around since cryptography.

Methods for Cracking Code

- Brute-Force Method
- Ciphertext-Only Method
- Known-Plaintext Method
- Chosen-Plaintext Method
- Chosen-Ciphertext Method
- Meet-in-the-Middle Method

Methods for Cracking Code - Brute-Force Attack

- An attacker tries every possible key with the decryption algorithm knowing that eventually one of them will work. All encryption algorithms are vulnerable to this attack.
- The objective of modern cryptographers is to have a keyspace large enough that it takes too much time (money) to accomplish a brute-force attack.
- For example: The best way to crack Caesar cipher-encrypted code is to use brute force.
  - There are only 25 possible rotations.
  - Therefore, it is not a big effort to try all possible rotations and see which one returns something that makes sense.

Methods for Cracking Code - Brute-Force Attack

- On average, a brute-force attack succeeds about 50 percent of the way through the keyspace, which is the set of all possible keys.
- A DES cracking machine recovered a 56-bit DES key in 22 hours using brute force.
- It is estimated it would take 149 trillion years to crack an AES key using the same method.

Methods for Cracking Code - Ciphertext-Only Attack

- An attacker has:
- The ciphertext of several messages, all of which have been encrypted using the same encryption algorithm, but the attacker has no knowledge of the underlying plaintext.
- The attacker could use statistical analysis to deduce the key.
- These kinds of attacks are no longer practical, because modern algorithms produce pseudorandom output that is resistant to statistical analysis.

Methods for Cracking Code - Known-Plaintext Attack

- An attacker has:
  - Access to the ciphertext of several messages.
  - Knowledge (underlying protocol, file type, or some characteristic strings) about the plaintext underlying that ciphertext.
- The attacker uses a brute-force attack to try keys until decryption with the correct key produces a meaningful result.
- Modern algorithms with enormous keyspaces make it unlikely for this attack to succeed, because, on average, an attacker must search through at least half of the keyspace to be successful.

Methods for Cracking Code - Chosen-Plaintext Attack

- An attacker chooses which data the encryption device encrypts and observes the ciphertext output. A chosen-plaintext attack is more powerful than a known-plaintext attack, because the chosen plaintext might yield more information about the key.
- This attack is not very practical, because it is often difficult or impossible to capture both the ciphertext and plaintext.

Methods for Cracking Code - Chosen-Ciphertext Attack

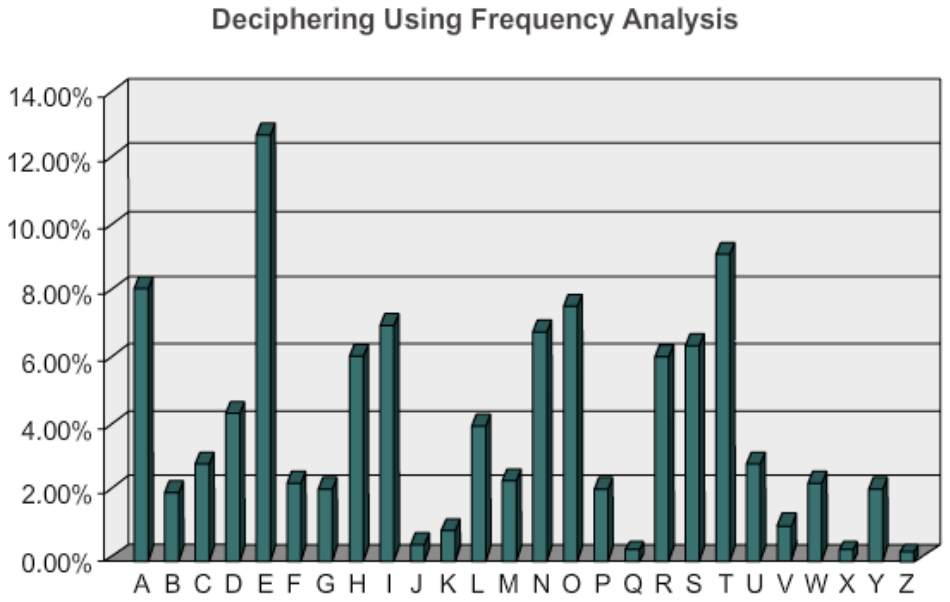
- An attacker chooses different ciphertext to be decrypted and has access to the decrypted plaintext. With the pair, the attacker can search through the keyspace and determine which key decrypts the chosen ciphertext in the captured plaintext.
- This attack is analogous to the chosen-plaintext attack.
  - Like the chosen-plaintext attack, this attack is not very practical.
  - Again, it is difficult or impossible for the attacker to capture both the ciphertext and plaintext.

Methods for Cracking Code - Meet-in-the-Middle

- The meet-in-the-middle attack is a known plaintext attack.
- The attacker knows that a portion of the plaintext and the corresponding ciphertext.
- The plaintext is encrypted with every possible key, and the results are stored. The ciphertext is then decrypted using every key, until one of the results matches one of the stored values.

Cracking Code Example

- The best way to crack the code is to use brute force.
- Because there are only 25 possible rotations, the effort is relatively small to try all possible rotations and see which one returns something that makes sense.
- A more scientific approach is to use the fact that some characters in the English alphabet are used more often than others.
- This method is called frequency analysis.



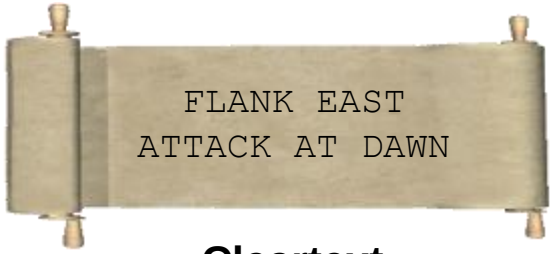
The graph outlines the frequency of letters in the English language.

For example, the letters E, T and A are the most popular.

Cracking Code Example- Frequency Analysis Method

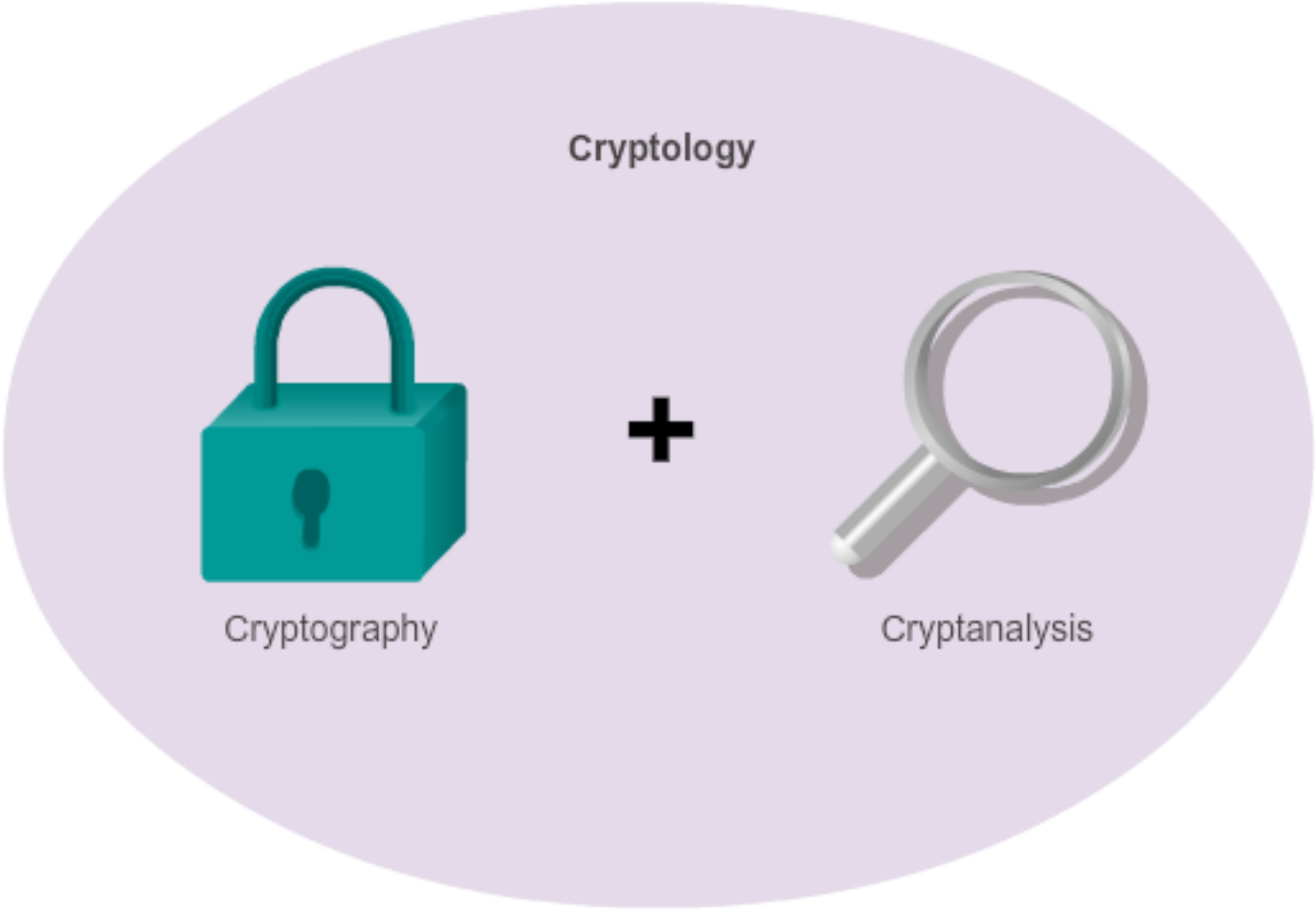
- The English alphabet is used more often than others.
  - E, T, and A are the most popular letters.
  - J, Q, X, and Z are the least popular.
- Caesar ciphered message:
  - The letter D appears six times.
  - The letter W appears four times.
  - Therefore, it is probable that they represent the more popular letters.
- In this case, D represents the letter A, and W represents the letter T.

Ciphered Text



Cleartext

Making and Breaking Secret Codes



Making and Breaking Secret Codes Cont.

- Cryptology is the science of making and breaking secret codes. It combines cryptography (development and use of codes), and cryptanalysis, (breaking of those codes).
- There is a symbiotic relationship between the two disciplines, because each makes the other one better.
  - National security organizations employ members of both disciplines and put them to work against each other.
- There have been times when one of the disciplines has been ahead of the other.
  - Currently, it is believed that cryptographers have the edge.

Cryptanalysis

- Ironically, it is impossible to prove an algorithm secure. It can only be proven that it is not vulnerable to known cryptanalytic attacks.
- There is a need for mathematicians, scholars, and security forensic experts to keep trying to break the encryption methods.
- Cryptanalysis are most used employed by:
  - Governments in military and diplomatic surveillance.
  - Enterprises in testing the strength of security procedures.

Sample Cryptanalysis Job Description

NSA

Cryptanalysis

National Security Agency | Fort Meade, MD

Job Description

Cryptanalysis is one of the core technical disciplines necessary for the NSA to accomplish its mission and provide critical intelligence to the nation's leaders. In an ever-changing global environment, the need for Cryptanalysts will remain constant.

Traditionally, Cryptanalysis is the art and science of solving cryptograms (writings in cipher or code) or cryptographic systems (devices for enciphering and deciphering) through analysis without prior knowledge of the encryption method. In a code, a word or phrase is replaced with another word, number, or symbol. In a cipher, each letter is replaced with another letter, number or symbol. Using known techniques and imagination, a Cryptanalyst systematically identifies basic elements in a cipher code that may lead to its solution. Modern Cryptanalysis includes analysis of any type of hidden information, whether a traditional cipher or a telecommunication protocol.

ANSWERING THE TOUGH QUESTIONS:

Cryptanalysts utilize mathematics, computer programming, engineering, and language skills as well as new technologies and creativity to solve tomorrow's problems today. That's why the NSA is looking for people who are intelligent and imaginative, and who can contribute original ideas to the solution of complex challenges. Cryptanalysts must communicate clearly, concentrate long and hard on difficult problems, and not be discouraged if success is elusive. No specific major is targeted for Cryptanalysis; the NSA hires people with technical and non-technical degrees, ranging from mathematics to music, engineering to history, and computer programming to chemistry.

The Secret Is in the Keys

- Authentication, integrity, and data confidentiality are implemented in many ways using various protocols and algorithms. Choice depends on the security level required in the security policy.

	Integrity	Authentication	Confidentiality
Common cryptographic hashes, protocols, and algorithms	MD5 (weaker) SHA (stronger)	HMAC-MD5 HMAC-SHA-1 RSA and DSA	DES (weaker) 3DES AES (stronger)

The Secret Is in the Keys Cont.

- Security of encryption lies in the secrecy of the keys, not the algorithm.
- Old encryption algorithms were based on the secrecy of the algorithm to achieve confidentiality.
- With modern technology, algorithm secrecy no longer matters since reverse engineering is often simple; therefore, public-domain algorithms are often used. Now, successful decryption requires knowledge of the keys.
- How can the keys be kept secret?

Questions?

End of Lecture 5