Cryptology

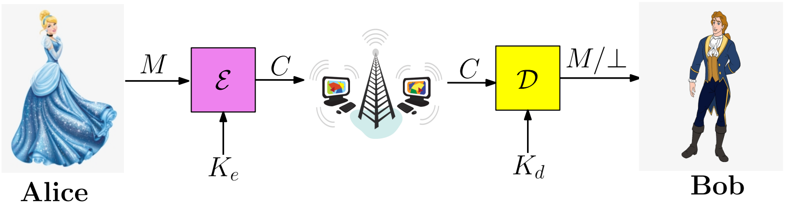
Sabyasachi Karati

Assistant Professor
Cryptology and Security Research Unit (C.S.R.U)
R. C. Bose Centre for Cryptology and Security
Indian Statistical Institute (ISI)
Kolkata, India

Lecture 02

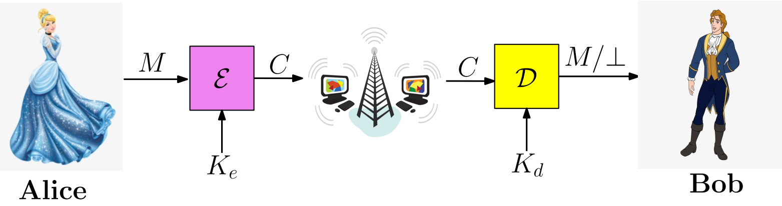
History and Classical Ciphers

Cryptographic Schemes



- $\mathcal{E}$: Encryption algorithm, and K_e: Encryption key.
- $\mathcal{D}$: Decryption algorithm, and K_d: Decryption key.
- M: Plain text or Message, and C: Cipher text or Encrypted message.

Cryptographic Schemes

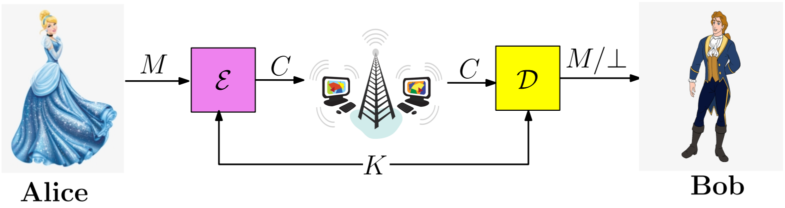


- $\mathcal{E}$: Encryption algorithm, and K_e: Encryption key.
- $\mathcal{D}$: Decryption algorithm, and K_d: Decryption key.
- M: Plain text or Message, and C: Cipher text or Encrypted message.

Settings

- Symmetric Key: $K_e = K_d$.
- Asymmetric Key or Public Key: $K_e \neq K_d$.

Cryptographic Schemes



Symmetric Encryption Scheme

Definition

Symmetric Encryption scheme is a three-tuple of algorithms $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ defined over a three-tuple of spaces $(\mathcal{K}, \mathcal{P}, \mathcal{C})$, where:

Symmetric Encryption Scheme

Definition

Symmetric Encryption scheme is a three-tuple of algorithms $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ defined over a three-tuple of spaces $(\mathcal{K}, \mathcal{P}, \mathcal{C})$, where:

- $\mathcal{P}$: Plaintext or Message Space, a finite set of possible plaintexts.
- $\mathcal{C}$: Cipher Space, a finite set of possible ciphertexts.
- $\mathcal{K}$: Key Space, a finite set of possible keys.

Symmetric Encryption Scheme

Definition

Symmetric Encryption scheme is a three-tuple of algorithms $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ defined over a three-tuple of spaces $(\mathcal{K}, \mathcal{P}, \mathcal{C})$, where:

- $\mathcal{P}$: Plaintext or Message Space, a finite set of possible plaintexts.
- $\mathcal{C}$: Cipher Space, a finite set of possible ciphertexts.
- $\mathcal{K}$: Key Space, a finite set of possible keys.
- $\mathcal{G}$: The Key-Generation Algorithm, a probabilistic algorithm that outputs a key k from $\mathcal{K}$ chosen according to some distribution.
- $\mathcal{E}$: The Encryption Algorithm,

$$\begin{aligned} \mathcal{E} \quad : \quad & \mathcal{K} \times \mathcal{P} \to \mathcal{C} \\ & \mathcal{E}(k, m) = c, \text{ where } k \in \mathcal{K}, m \in \mathcal{P}, c \in \mathcal{C}. \end{aligned}$$

- $\mathcal{D}$: The Decryption Algorithm,

$$\begin{aligned} \mathcal{D} \quad : \quad & \mathcal{K} \times \mathcal{C} \to \mathcal{P} \\ & \mathcal{D}(k, c) = m, \text{ where } k \in \mathcal{K}, m \in \mathcal{P}, c \in \mathcal{C}. \end{aligned}$$

Basic Correctness of a Symmetric Encryption Scheme

For all key $k \in \mathcal{K}$ generated by $\mathcal{G}$ and for all plaintext $m \in \mathcal{P}$, the following must hold:

$$\mathcal{D}(k, \mathcal{E}(k, m)) = m.$$

Symmetric Encryption Scheme

Basic Correctness of a Symmetric Encryption Scheme

For all key $k \in \mathcal{K}$ generated by $\mathcal{G}$ and for all plaintext $m \in \mathcal{P}$, the following must hold:

$$\mathcal{D}(k, \mathcal{E}(k, m)) = m.$$

- Decrypting a ciphertext using the appropriate key yields the original message that was encrypted.

Kerckhoffs' Principle

- In 1883, Auguste Kerckhoffs postulates that

Definition (Kerckhoffs' Principle)

A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms.

Kerckhoffs' Principle

- In 1883, Auguste Kerckhoffs postulates that

Definition (Kerckhoffs' Principle)

A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms.

Arguments in favour of Kerckhoffs' Principle

1. It is easy to maintain secrecy of a small key or to share a small key.

Kerckhoffs' Principle

- In 1883, Auguste Kerckhoffs postulates that

Definition (Kerckhoffs' Principle)

A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms.

Arguments in favour of Kerckhoffs' Principle

1. It is easy to maintain secrecy of a small key or to share a small key.
2. If key is leaked, then communicating parties can keep on using the same algorithm with different key.

Kerckhoffs' Principle

- In 1883, Auguste Kerckhoffs postulates that

Definition (Kerckhoffs' Principle)

A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms.

Arguments in favour of Kerckhoffs' Principle

1. It is easy to maintain secrecy of a small key or to share a small key.
2. If key is leaked, then communicating parties can keep on using the same algorithm with different key.
3. In case of many pairs are communicating, it is easy to have same algorithm for all the pairs with different keys than different algorithms for each pair.

Kerckhoffs' Principle

- In 1883, Auguste Kerckhoffs postulates that

Definition (Kerckhoffs' Principle)

A cryptosystem should be secure even if the attacker knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms.

Arguments in favour of Kerckhoffs' Principle

1. It is easy to maintain secrecy of a small key or to share a small key.
2. If key is leaked, then communicating parties can keep on using the same algorithm with different key.
3. In case of many pairs are communicating, it is easy to have same algorithm for all the pairs with different keys than different algorithms for each pair.

Therefore, Kerckhoffs' principle demands that everything (algorithm) is public except for the key.

Kerckhoffs' Principle

Advantage of Open Cryptographic Design

1. They undergo public scrutiny and are therefore likely to be stronger.
   - it is very difficult to construct good cryptographic schemes.
   - if it has been extensively studied (by experts other than the designers of the scheme themselves) and no weaknesses have been found, then our confidence in the security of a scheme will be much higher.

Advantage of Open Cryptographic Design

1. They undergo public scrutiny and are therefore likely to be stronger.
   - it is very difficult to construct good cryptographic schemes.
   - if it has been extensively studied (by experts other than the designers of the scheme themselves) and no weaknesses have been found, then our confidence in the security of a scheme will be much higher.
2. It is better for security flaws, if they exist, to be revealed by " ethical hackers" (leading, hopefully, to the system being fixed) rather than having these flaws be known only to malicious parties.

Kerckhoffs' Principle

Advantage of Open Cryptographic Design

1. They undergo public scrutiny and are therefore likely to be stronger.
    - it is very difficult to construct good cryptographic schemes.
    - if it has been extensively studied (by experts other than the designers of the scheme themselves) and no weaknesses have been found, then our confidence in the security of a scheme will be much higher.
2. It is better for security flaws, if they exist, to be revealed by " ethical hackers" (leading, hopefully, to the system being fixed) rather than having these flaws be known only to malicious parties.
3. If the security of the system relies on the secrecy of the algorithm, then reverse engineering of the code (or leakage by industrial espionage) poses a serious threat to security.

Kerckhoffs' Principle

Advantage of Open Cryptographic Design

1. They undergo public scrutiny and are therefore likely to be stronger.
   - it is very difficult to construct good cryptographic schemes.
   - if it has been extensively studied (by experts other than the designers of the scheme themselves) and no weaknesses have been found, then our confidence in the security of a scheme will be much higher.
2. It is better for security flaws, if they exist, to be revealed by " ethical hackers" (leading, hopefully, to the system being fixed) rather than having these flaws be known only to malicious parties.
3. If the security of the system relies on the secrecy of the algorithm, then reverse engineering of the code (or leakage by industrial espionage) poses a serious threat to security.
4. Public design enables the establishment of standards.

Kerckhoffs' Principle

Advantage of Open Cryptographic Design

1. They undergo public scrutiny and are therefore likely to be stronger.
   - it is very difficult to construct good cryptographic schemes.
   - if it has been extensively studied (by experts other than the designers of the scheme themselves) and no weaknesses have been found, then our confidence in the security of a scheme will be much higher.
2. It is better for security flaws, if they exist, to be revealed by " ethical hackers" (leading, hopefully, to the system being fixed) rather than having these flaws be known only to malicious parties.
3. If the security of the system relies on the secrecy of the algorithm, then reverse engineering of the code (or leakage by industrial espionage) poses a serious threat to security.
4. Public design enables the establishment of standards.

Importance of Kerckhoffs' Principle through Example

Content Scrambling System (CSS) for DVD content protection, which was broken easily once it was reverse-engineered.

Attack Models

There are four commonly considered attack models:

1. Ciphertext-only attack
2. Known-plaintext attack
3. Chosen-plaintext attack
4. Chosen-ciphertext attack

Attack Models

Ciphertext-only attack

- **Given:** Only Ciphertext(s): $\{c_i \mid 1 \leqslant i \leqslant n\}$ encrypted under the same key k.

Attack Models

Ciphertext-only attack

- **Given:** Only Ciphertext(s): $\{c_i \mid 1 \leqslant i \leqslant n\}$ encrypted under the same key k.
- **Goal:** Find (one of) the message(s) m^* such that corresponding $c^* \in \{c_i \mid 1 \leqslant i \leqslant n\}$ and/or the key k.

Attack Models

Ciphertext-only attack

- **Given:** Only Ciphertext(s): $\{c_i \mid 1 \leqslant i \leqslant n\}$ encrypted under the same key k.
- **Goal:** Find (one of) the message(s) m^* such that corresponding $c^* \in \{c_i \mid 1 \leqslant i \leqslant n\}$ and/or the key k.
- **Weaker Goal:** Find some information regarding the key k.

Attack Models

Known-plaintext attack

- **Given:** One or more plaintext-ciphertext pairs $\{(m_i, c_i) \mid 1 \leqslant i \leqslant n\}$ encrypted under the same key k.

Known-plaintext attack

- **Given:** One or more plaintext-ciphertext pairs $\{(m_i, c_i) \mid 1 \leqslant i \leqslant n\}$ encrypted under the same key k.
- **Goal:** Find a valid plaintext m^* for a new c^*, that is $c^* \notin \{c_i \mid 1 \leqslant i \leqslant n\}$, under the key k and/or the key k.

Known-plaintext attack

- **Given:** One or more plaintext-ciphertext pairs $\{(m_i, c_i) \mid 1 \leqslant i \leqslant n\}$ encrypted under the same key k.
- **Goal:** Find a valid plaintext m^* for a new c^*, that is $c^* \notin \{c_i \mid 1 \leqslant i \leqslant n\}$, under the key k and/or the key k.
- **Weaker Goal:** Find some information regarding the key k.

Attack Models

Chosen-plaintext attack

- **Given:**
  - Adversary has the temporary access to the $\mathcal{E}(k, \cdot)$ for some unknown key $k \in \mathcal{K}$.

Attack Models

Chosen-plaintext attack

- **Given:**
  - Adversary has the temporary access to the $\mathcal{E}(k, \cdot)$ for some unknown key $k \in \mathcal{K}$.
  - Adversary chooses a set of plain texts $\{m_i \mid 1 \leqslant i \leqslant n\}$.

Chosen-plaintext attack

- **Given:**
  - Adversary has the temporary access to the $\mathcal{E}(k, \cdot)$ for some unknown key $k \in \mathcal{K}$.
  - Adversary chooses a set of plain texts $\{m_i \mid 1 \leqslant i \leqslant n\}$.
  - Receives the corresponding ciphertexts $\{c_i \mid 1 \leqslant i \leqslant n\}$ such that $c_i = \mathcal{E}(k, m_i)\ \forall i$.

Attack Models

Chosen-plaintext attack

- **Given:**
  - Adversary has the temporary access to the $\mathcal{E}(k, \cdot)$ for some unknown key $k \in \mathcal{K}$.
  - Adversary chooses a set of plain texts $\{m_i \mid 1 \leqslant i \leqslant n\}$.
  - Receives the corresponding ciphertexts $\{c_i \mid 1 \leqslant i \leqslant n\}$ such that $c_i = \mathcal{E}(k, m_i)\ \forall i$.
- **Goal:** Find a valid plaintext m^* for a new c^*, that is $c^* \notin \{c_i \mid 1 \leqslant i \leqslant n\}$, under the key k and/or the key k.

Attack Models

Chosen-plaintext attack

- **Given:**
  - Adversary has the temporary access to the $\mathcal{E}(k, \cdot)$ for some unknown key $k \in \mathcal{K}$.
  - Adversary chooses a set of plain texts $\{m_i \mid 1 \leqslant i \leqslant n\}$.
  - Receives the corresponding ciphertexts $\{c_i \mid 1 \leqslant i \leqslant n\}$ such that $c_i = \mathcal{E}(k, m_i)\ \forall i$.
- **Goal:** Find a valid plaintext m^* for a new c^*, that is $c^* \notin \{c_i \mid 1 \leqslant i \leqslant n\}$, under the key k and/or the key k.
- **Weaker Goal:** Find some information regarding the key k.

Chosen-ciphertext attack

- **Given:**
  - Adversary has the temporary access to the $\mathcal{D}(k, \cdot)$ for some unknown key $k \in \mathcal{K}$.

Chosen-ciphertext attack

- **Given:**
  - Adversary has the temporary access to the $\mathcal{D}(k, \cdot)$ for some unknown key $k \in \mathcal{K}$.
  - Adversary chooses a set of ciphertexts $\{c_i \mid 1 \leqslant i \leqslant n\}$.

Chosen-ciphertext attack

- **Given:**
  - Adversary has the temporary access to the $\mathcal{D}(k, \cdot)$ for some unknown key $k \in \mathcal{K}$.
  - Adversary chooses a set of ciphertexts $\{c_i \mid 1 \leqslant i \leqslant n\}$.
  - Receives the corresponding plaintexts $\{m_i \mid 1 \leqslant i \leqslant n\}$ such that $m_i = \mathcal{D}(k, c_i)\ \forall i$.

Attack Models

Chosen-ciphertext attack

- **Given:**
  - Adversary has the temporary access to the $\mathcal{D}(k, \cdot)$ for some unknown key $k \in \mathcal{K}$.
  - Adversary chooses a set of ciphertexts $\{c_i \mid 1 \leqslant i \leqslant n\}$.
  - Receives the corresponding plaintexts $\{m_i \mid 1 \leqslant i \leqslant n\}$ such that $m_i = \mathcal{D}(k, c_i)\ \forall i$.
- **Goal:** Find a valid plaintext m^* for a new c^*, that is $c^* \notin \{c_i \mid 1 \leqslant i \leqslant n\}$, under the key k and/or the key k.

Chosen-ciphertext attack

- **Given:**
  - Adversary has the temporary access to the $\mathcal{D}(k,\cdot)$ for some unknown key $k \in \mathcal{K}$.
  - Adversary chooses a set of ciphertexts $\{c_i \mid 1 \leqslant i \leqslant n\}$.
  - Receives the corresponding plaintexts $\{m_i \mid 1 \leqslant i \leqslant n\}$ such that $m_i = \mathcal{D}(k, c_i)\ \forall i$.
- **Goal:** Find a valid plaintext m^* for a new c^*, that is $c^* \notin \{c_i \mid 1 \leqslant i \leqslant n\}$, under the key k and/or the key k.
- **Weaker Goal:** Find some information regarding the key k.

History of Classical Ciphers

- Some examples of historical ciphers and show that they are all badly broken.

History of Classical Ciphers

- Some examples of historical ciphers and show that they are all badly broken.
- **Goal:**
  1. To highlight the weaknesses of ad-hoc approaches.

History of Classical Ciphers

- Some examples of historical ciphers and show that they are all badly broken.
- **Goal:**
  1. To highlight the weaknesses of ad-hoc approaches.
  2. Motivation towards a more modern and rigorous approach.

History of Classical Ciphers

- Some examples of historical ciphers and show that they are all badly broken.
- **Goal:**
  1. To highlight the weaknesses of ad-hoc approaches.
  2. Motivation towards a more modern and rigorous approach.
  3. Demonstrate that simple approaches to achieving secure encryption are unlikely to succeed.

History of Classical Ciphers

- Some examples of historical ciphers and show that they are all badly broken.
- **Goal:**
  1. To highlight the weaknesses of ad-hoc approaches.
  2. Motivation towards a more modern and rigorous approach.
  3. Demonstrate that simple approaches to achieving secure encryption are unlikely to succeed.
  4. To identify/learn why that is the case.

Caesar's Cipher (100 B.C. - 44 B.C.)

- It is one of the oldest recorded ciphers.
- Is described in De Vita Caesarum, Divus Iulius (The Lives of the Caesars, The Deified Julius) which was written in approximately 110 C.E.:

> "There are also letters of his to Cicero, as well as to his intimates on private affairs, and in the latter, if he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. *If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others*."

Caesar's Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, Z\}$ (English Alphabet)

Caesar's Cipher (100 B.C. - 44 B.C.)

Caesar's Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, Z\}$ (English Alphabet) $= \{0, 1, 2, \ldots, 25\} = \mathbb{Z}_{26}$.

A	B	C	D	$\cdots$	W	X	Y	Z
0	1	2	3	$\cdots$	22	23	24	25

Caesar's Cipher (100 B.C. - 44 B.C.)

Caesar's Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, Z\}$ (English Alphabet) $= \{0, 1, 2, \ldots, 25\} = \mathbb{Z}_{26}$.

A	B	C	D	$\cdots$	W	X	Y	Z
0	1	2	3	$\cdots$	22	23	24	25

- $\mathcal{E} : c := (m + 3) \pmod{26}$.

A	B	C	D	$\cdots$	W	X	Y	Z
D	E	F	G	$\cdots$	Z	A	B	C

Caesar's Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, Z\}$ (English Alphabet) $= \{0, 1, 2, \ldots, 25\} = \mathbb{Z}_{26}$.

A	B	C	D	$\cdots$	W	X	Y	Z
0	1	2	3	$\cdots$	22	23	24	25

- $\mathcal{E} : c := (m+3) \pmod{26}$.

A	B	C	D	$\cdots$	W	X	Y	Z
D	E	F	G	$\cdots$	Z	A	B	C

- $\mathcal{D} : m := (c-3) \pmod{26}$.

A	B	C	D	$\cdots$	W	X	Y	Z
X	Y	Z	A	$\cdots$	T	U	V	W

Caesar's Cipher (100 B.C. - 44 B.C.)

Example

A	B	C	D	$\cdots$	W	X	Y	Z
D	E	F	G	$\cdots$	Z	A	B	C

- **Plaintext:** BEGIN THE ATTACK NOW.

Caesar's Cipher (100 B.C. - 44 B.C.)

Example

A	B	C	D	$\cdots$	W	X	Y	Z
D	E	F	G	$\cdots$	Z	A	B	C

- **Plaintext:** BEGIN THE ATTACK NOW.
- **Ciphertext:** EHJLQ WKH DWWDFN QRZ.

Drawback

- Fixed Key, in other words, The method is fixed.

Caesar's Cipher (100 B.C. - 44 B.C.)

Example

A	B	C	D	$\cdots$	W	X	Y	Z
D	E	F	G	$\cdots$	Z	A	B	C

- **Plaintext:** BEGIN THE ATTACK NOW.
- **Ciphertext:** EHJLQ WKH DWWDFN QRZ.

Drawback

- Fixed Key, in other words, The method is fixed.
- If the encryption scheme is made public then decryption is trivial.

Caesar's Cipher (100 B.C. - 44 B.C.)

Example

A	B	C	D	$\cdots$	W	X	Y	Z
D	E	F	G	$\cdots$	Z	A	B	C

- **Plaintext:** BEGIN THE ATTACK NOW.
- **Ciphertext:** EHJLQ WKH DWWDFN QRZ.

Drawback

- Fixed Key, in other words, The method is fixed.
- If the encryption scheme is made public then decryption is trivial.
- $\mathcal{G}$: Does nothing!

Caesar's Cipher (100 B.C. - 44 B.C.)

Example

A	B	C	D	$\cdots$	W	X	Y	Z
D	E	F	G	$\cdots$	Z	A	B	C

- **Plaintext:** BEGIN THE ATTACK NOW.
- **Ciphertext:** EHJLQ WKH DWWDFN QRZ.

Drawback

- Fixed Key, in other words, The method is fixed.
- If the encryption scheme is made public then decryption is trivial.
- $\mathcal{G}$: Does nothing!

Does not follow Kerckhoffs' Principle.

Shift Cipher

Shift Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, Z\}$ (English Alphabet) $= \mathbb{Z}_{26}$.
- $\mathcal{K} = \mathbb{Z}_{26}$.

Shift Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, Z\}$ (English Alphabet) $= \mathbb{Z}_{26}$.
- $\mathcal{K} = \mathbb{Z}_{26}$.
- $\mathcal{G} : k \xleftarrow{R} \mathbb{Z}_{26}$

Shift Cipher

Shift Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, Z\}$ (English Alphabet) $= \mathbb{Z}_{26}$.
- $\mathcal{K} = \mathbb{Z}_{26}$.
- $\mathcal{G} : k \xleftarrow{R} \mathbb{Z}_{26}$
- $\mathcal{E} : c := (m + k) \pmod{26}$.

Shift Cipher

Shift Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, Z\}$ (English Alphabet) $= \mathbb{Z}_{26}$.
- $\mathcal{K} = \mathbb{Z}_{26}$.
- $\mathcal{G} : k \xleftarrow{R} \mathbb{Z}_{26}$
- $\mathcal{E} : c := (m + k) \pmod{26}$.
- $\mathcal{D} : m := (c - k) \pmod{26}$.

Shift Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, Z\}$ (English Alphabet) $= \mathbb{Z}_{26}$.
- $\mathcal{K} = \mathbb{Z}_{26}$.
- $\mathcal{G} : k \xleftarrow{R} \mathbb{Z}_{26}$
- $\mathcal{E} : c := (m + k) \pmod{26}$.
- $\mathcal{D} : m := (c - k) \pmod{26}$.

Caesar's Cipher is a special case of Shift cipher with $K = 3$

Shift Cipher

Example

- Let $K = 7$

A	B	C	D	E	F	G	H	I	J	K	L	M
H	I	J	K	L	M	N	O	P	Q	R	S	T

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

Example

- Let $K = 7$

A	B	C	D	E	F	G	H	I	J	K	L	M
H	I	J	K	L	M	N	O	P	Q	R	S	T

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

- **Plaintext:** BEGIN THE ATTACK NOW.

Shift Cipher

Example

- Let $K = 7$

A	B	C	D	E	F	G	H	I	J	K	L	M
H	I	J	K	L	M	N	O	P	Q	R	S	T

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

- **Plaintext:** BEGIN THE ATTACK NOW.
- **Ciphertext:** ILNPU AOL HAAHJR UVD.

Shift Cipher

Cryptanalysis of Shift Cipher

- Is it secure? Answer: No

Shift Cipher

Cryptanalysis of Shift Cipher

- Is it secure? Answer: No
- Is it possible to decrypt a message without knowing the key? Answer: Yes

Shift Cipher

Cryptanalysis of Shift Cipher

- Is it secure? Answer: No
- Is it possible to decrypt a message without knowing the key? Answer: Yes
- **Brute-forced Attack:**
  - Check each key one after another.
  - Stop when the text makes some sense.

Cryptanalysis of Shift Cipher

- Is it secure? Answer: No
- Is it possible to decrypt a message without knowing the key? Answer: Yes
- **Brute-forced Attack:**
  - Check each key one after another.
  - Stop when the text makes some sense.

K	Decrypted Text	Make Sense?
0	ILNPU AOL HAAHJR UVD	No

Shift Cipher

Cryptanalysis of Shift Cipher

- Is it secure? Answer: No
- Is it possible to decrypt a message without knowing the key? Answer: Yes
- **Brute-forced Attack:**
  - Check each key one after another.
  - Stop when the text makes some sense.

K	Decrypted Text	Make Sense?
0	ILNPU AOL HAAHJR UVD	No
1	HKMOT ZNK GZZGIQ TUC	No

Cryptanalysis of Shift Cipher

- Is it secure? Answer: No
- Is it possible to decrypt a message without knowing the key? Answer: Yes
- **Brute-forced Attack:**
  - Check each key one after another.
  - Stop when the text makes some sense.

K	Decrypted Text	Make Sense?
0	ILNPU AOL HAAHJR UVD	No
1	HKMOT ZNK GZZGIQ TUC	No
2	GJLNS YMJ FYYFHP STB	No

Shift Cipher

Cryptanalysis of Shift Cipher

- Is it secure? Answer: No
- Is it possible to decrypt a message without knowing the key? Answer: Yes
- **Brute-forced Attack:**
  - Check each key one after another.
  - Stop when the text makes some sense.

K	Decrypted Text	Make Sense?
0	ILNPU AOL HAAHJR UVD	No
1	HKMOT ZNK GZZGIQ TUC	No
2	GJLNS YMJ FYYFHP STB	No
3	FIKMR XLI EXXEGO RSA	No

Shift Cipher

Cryptanalysis of Shift Cipher

- Is it secure? Answer: No
- Is it possible to decrypt a message without knowing the key? Answer: Yes
- **Brute-forced Attack:**
  - Check each key one after another.
  - Stop when the text makes some sense.

K	Decrypted Text	Make Sense?
0	ILNPU AOL HAAHJR UVD	No
1	HKMOT ZNK GZZGIQ TUC	No
2	GJLNS YMJ FYYFHP STB	No
3	FIKMR XLI EXXEGO RSA	No
4	EHJLQ WKH DWWDFN QRZ	No

Cryptanalysis of Shift Cipher

- Is it secure? Answer: No
- Is it possible to decrypt a message without knowing the key? Answer: Yes
- **Brute-forced Attack:**
  - Check each key one after another.
  - Stop when the text makes some sense.

K	Decrypted Text	Make Sense?
0	ILNPU AOL HAAHJR UVD	No
1	HKMOT ZNK GZZGIQ TUC	No
2	GJLNS YMJ FYYFHP STB	No
3	FIKMR XLI EXXEGO RSA	No
4	EHJLQ WKH DWWDFN QRZ	No
5	DGIKP VJG CVVCEM PQY	No

Cryptanalysis of Shift Cipher

- Is it secure? Answer: No
- Is it possible to decrypt a message without knowing the key? Answer: Yes
- **Brute-forced Attack:**
  - Check each key one after another.
  - Stop when the text makes some sense.

K	Decrypted Text	Make Sense?
0	ILNPU AOL HAAHJR UVD	No
1	HKMOT ZNK GZZGIQ TUC	No
2	GJLNS YMJ FYYFHP STB	No
3	FIKMR XLI EXXEGO RSA	No
4	EHJLQ WKH DWWDFN QRZ	No
5	DGIKP VJG CVVCEM PQY	No
6	CFHJO UIF BUUBDL OPX	No

Cryptanalysis of Shift Cipher

- Is it secure? Answer: No
- Is it possible to decrypt a message without knowing the key? Answer: Yes
- **Brute-forced Attack:**
  - Check each key one after another.
  - Stop when the text makes some sense.

K	Decrypted Text	Make Sense?
0	ILNPU AOL HAAHJR UVD	No
1	HKMOT ZNK GZZGIQ TUC	No
2	GJLNS YMJ FYYFHP STB	No
3	FIKMR XLI EXXEGO RSA	No
4	EHJLQ WKH DWWDFN QRZ	No
5	DGIKP VJG CVVCEM PQY	No
6	CFHJO UIF BUUBDL OPX	No
7	BEGIN THE ATTACK NOW	Yes

Cryptanalysis of Shift Cipher

- Is it secure? Answer: No
- Is it possible to decrypt a message without knowing the key? Answer: Yes
- **Brute-forced Attack:**
  - Check each key one after another.
  - Stop when the text makes some sense.

K	Decrypted Text	Make Sense?
0	ILNPU AOL HAAHJR UVD	No
1	HKMOT ZNK GZZGIQ TUC	No
2	GJLNS YMJ FYYFHP STB	No
3	FIKMR XLI EXXEGO RSA	No
4	EHJLQ WKH DWWDFN QRZ	No
5	DGIKP VJG CVVCEM PQY	No
6	CFHJO UIF BUUBDL OPX	No
7	BEGIN THE ATTACK NOW	Yes
	Stop	

Shift Cipher

Cryptanalysis of Shift Cipher

- Is it secure? Answer: No
- Is it possible to decrypt a message without knowing the key? Answer: Yes
- **Brute-forced Attack:**
  - Check each key one after another.
  - Stop when the text makes some sense.

K	Decrypted Text	Make Sense?
0	ILNPU AOL HAAHJR UVD	No
1	HKMOT ZNK GZZGIQ TUC	No
2	GJLNS YMJ FYYFHP STB	No
3	FIKMR XLI EXXEGO RSA	No
4	EHJLQ WKH DWWDFN QRZ	No
5	DGIKP VJG CVVCEM PQY	No
6	CFHJO UIF BUUBDL OPX	No
7	BEGIN THE ATTACK NOW	Yes
	Stop	

- Maximum number of tries required?

Cryptanalysis of Shift Cipher

- Is it secure? Answer: No
- Is it possible to decrypt a message without knowing the key? Answer: Yes
- **Brute-forced Attack:**
  - Check each key one after another.
  - Stop when the text makes some sense.

K	Decrypted Text	Make Sense?
0	ILNPU AOL HAAHJR UVD	No
1	HKMOT ZNK GZZGIQ TUC	No
2	GJLNS YMJ FYYFHP STB	No
3	FIKMR XLI EXXEGO RSA	No
4	EHJLQ WKH DWWDFN QRZ	No
5	DGIKP VJG CVVCEM PQY	No
6	CFHJO UIF BUUBDL OPX	No
7	BEGIN THE ATTACK NOW	Yes
	Stop	

- Maximum number of tries required? 26

Shift Cipher

- Should not be vulnerable to such a brute-force attack.
- Else, it can be completely broken, irrespective of how sophisticated the encryption algorithm is.
- **Sufficient key space principle:** For secure encryption schemes the key space must not be vulnerable to exhaustive search.

Shift Cipher

- Should not be vulnerable to such a brute-force attack.
- Else, it can be completely broken, irrespective of how sophisticated the encryption algorithm is.
- **Sufficient key space principle:** For secure encryption schemes the key space must not be vulnerable to exhaustive search.
  Note: Only true if $|\mathcal{P}| \geqslant |\mathcal{K}|$.

Shift Cipher

- Should not be vulnerable to such a brute-force attack.
- Else, it can be completely broken, irrespective of how sophisticated the encryption algorithm is.
- **Sufficient key space principle:** For secure encryption schemes the key space must not be vulnerable to exhaustive search.
  Note: Only true if $|\mathcal{P}| \geqslant |\mathcal{K}|$.
- **Present Standard:** $|\mathcal{K}| \geq 2^{80}$.

- Should not be vulnerable to such a brute-force attack.
- Else, it can be completely broken, irrespective of how sophisticated the encryption algorithm is.
- **Sufficient key space principle:** For secure encryption schemes the key space must not be vulnerable to exhaustive search.
  Note: Only true if $|\mathcal{P}| \geqslant |\mathcal{K}|$.
- **Present Standard:** $|\mathcal{K}| \geq 2^{80}$.
- **Note:** The above principle gives a *necessary condition* for security, not a sufficient one.

- Should not be vulnerable to such a brute-force attack.
- Else, it can be completely broken, irrespective of how sophisticated the encryption algorithm is.
- **Sufficient key space principle:** For secure encryption schemes the key space must not be vulnerable to exhaustive search.
  Note: Only true if $|\mathcal{P}| \geqslant |\mathcal{K}|$.
- **Present Standard:** $|\mathcal{K}| \geq 2^{80}$.
- **Note:** The above principle gives a *necessary condition* for security, not a sufficient one.
- Our next scheme has a *very large key space* but is still insecure.

Substitute Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, Z\}$ (English Alphabet).
- $\mathcal{K} = \Pi$ = All possible permutations of the symbols $\{A, B, C, \ldots, Z\}$.

Substitute Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, Z\}$ (English Alphabet).
- $\mathcal{K} = \Pi$ = All possible permutations of the symbols $\{A, B, C, \ldots, Z\}$.
- $\mathcal{G} : \pi \xleftarrow{R} \Pi$

Substitute Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, Z\}$ (English Alphabet).
- $\mathcal{K} = \Pi =$ All possible permutations of the symbols $\{A, B, C, \ldots, Z\}$.
- $\mathcal{G} : \pi \xleftarrow{R} \Pi$
- $\mathcal{E} : c := \pi(m)$.

Substitute Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, Z\}$ (English Alphabet).
- $\mathcal{K} = \Pi =$ All possible permutations of the symbols $\{A, B, C, \ldots, Z\}$.
- $\mathcal{G} : \pi \xleftarrow{R} \Pi$
- $\mathcal{E} : c := \pi(m)$.
- $\mathcal{D} : m := \pi^{-1}(c)$.

Substitute Cipher

Example

π :

A	B	C	D	E	F	G	H	I	J	K	L	M
H	I	J	K	L	M	N	O	P	Q	R	S	T

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

Substitute Cipher

Example

π :

A	B	C	D	E	F	G	H	I	J	K	L	M
H	I	J	K	L	M	N	O	P	Q	R	S	T

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

- **Plaintext:** BEGIN THE ATTACK NOW.

Substitute Cipher

Example

π :

A	B	C	D	E	F	G	H	I	J	K	L	M
H	I	J	K	L	M	N	O	P	Q	R	S	T

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

- **Plaintext:** BEGIN THE ATTACK NOW.
- **Ciphertext:** $\pi(\mathrm{B})\pi(\mathrm{E})\pi(\mathrm{G})\cdots$ = ILNPU AOL HAAHJR UVD.

Substitute Cipher

- The Shift Cipher is a special case of the Substitution Cipher.
    - The Shift Cipher includes only 26 of the 26! possible permutations of 26 elements.

Substitute Cipher

- The Shift Cipher is a special case of the Substitution Cipher.
  - The Shift Cipher includes only 26 of the 26! possible permutations of 26 elements.
- In both the Shift Cipher and the Substitution Cipher, once a key is chosen, each alphabetic character is mapped to a unique alphabetic character. These type of cryptosystems are called monoalphabetic cryptosystems.

Cryptanalysis of Substitute Cipher

Assumptions

- English-language text is being encrypted.
- The text is in grammatically-correct English.

Cryptanalysis of Substitute Cipher

Assumptions

- English-language text is being encrypted.
- The text is in grammatically-correct English.

Attack Idea

- Use statistical patterns of the English language.
  Note: The same attack works for any language.

Cryptanalysis of Substitute Cipher

Assumptions

- English-language text is being encrypted.
- The text is in grammatically-correct English.

Attack Idea

- Use statistical patterns of the English language.
  Note: The same attack works for any language.
- The attack utilizes the following two properties of the cipher:
  1. The mapping of each letter is fixed, that is, $e \mapsto L$ for all occurrences of e in the plaintext.
  2. The probability distribution of individual letters is known.
     - The average frequency counts of the different English letters are quite invariant over different texts.

Statistical Properties of English Language

- Relative Frequencies of the 26 letters.
- Compiled from numerous novels, magazines and newspaper.
- The following table was obtained by Beker and Piper.

Statistical Properties of English Language

- Relative Frequencies of the 26 letters.
- Compiled from numerous novels, magazines and newspaper.
- The following table was obtained by Beker and Piper.

Letter	Probability	Letter	Probability
A	0.082	N	0.067
B	0.015	O	0.075
C	0.028	P	0.019
D	0.043	Q	0.001
E	0.127	R	0.060
F	0.022	S	0.063
G	0.020	T	0.091
H	0.061	U	0.028
I	0.070	V	0.010
J	0.002	W	0.023
K	0.008	X	0.001
L	0.040	Y	0.020
M	0.024	Z	0.001

Statistical Properties of English Language

- Statistical analysis gives us the following partition the 26 letters into five groups:
  - E: Having probability of about 0.120.
  - T, A, O, I, N, S, H, R: Probability between 0.06 and 0.09.
  - D, L: Probability around 0.04.
  - C, U, M, W, F, G, Y, P, B: Prob. between 0.015 and 0.028.
  - V, K, J, X, Q, Z: Probability less than 0.01.

Cryptanalysis of Substitute Cipher

Statistical Properties of English Language

- Statistical analysis gives us the following partition the 26 letters into five groups:
  - E: Having probability of about 0.120.
  - T, A, O, I, N, S, H, R: Probability between 0.06 and 0.09.
  - D, L: Probability around 0.04.
  - C, U, M, W, F, G, Y, P, B: Prob. between 0.015 and 0.028.
  - V, K, J, X, Q, Z: Probability less than 0.01.
- It is also useful to consider distributions digrams and trigrams.

Statistical Properties of English Language

- Statistical analysis gives us the following partition the 26 letters into five groups:
  - E: Having probability of about 0.120.
  - T, A, O, I, N, S, H, R: Probability between 0.06 and 0.09.
  - D, L: Probability around 0.04.
  - C, U, M, W, F, G, Y, P, B: Prob. between 0.015 and 0.028.
  - V, K, J, X, Q, Z: Probability less than 0.01.
- It is also useful to consider distributions digrams and trigrams.
- Some of the most common diagrams (in decreasing order) are
  - TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF.

Cryptanalysis of Substitute Cipher

Statistical Properties of English Language

- Statistical analysis gives us the following partition the 26 letters into five groups:
  - E: Having probability of about 0.120.
  - T, A, O, I, N, S, H, R: Probability between 0.06 and 0.09.
  - D, L: Probability around 0.04.
  - C, U, M, W, F, G, Y, P, B: Prob. between 0.015 and 0.028.
  - V, K, J, X, Q, Z: Probability less than 0.01.
- It is also useful to consider distributions digrams and trigrams.
- Some of the most common diagrams (in decreasing order) are
  - TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF.
- Some of the most common trigrams (in decreasing order) are
  - THE, ING, AND, HER, ERE, ENT, THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH.

Ciphertext:

YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJNDIFEFMDZCDM
QZKCEYFCJMYRNCWJCSZREXCHZUNMXZNZUCDRJXYYSMRTMEYIFZWDYVZ
VYFZUMRZCRWNZDZJJXZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR

Cryptanalysis of Substitute Cipher

Ciphertext:
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJNDIFEFMDZCDM
QZKCEYFCJMYRNCWJCSZREXCHZUNMXZNZUCDRJXYYSMRTMEYIFZWDYVZ
VYFZUMRZCRWNZDZJJXZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR

- Tabulate the frequency distribution of characters:
  A appeared 0 times, B appeared 1 times, and so on
- Compare them with the known frequencies of English text.
- Guess parts of the mapping based on the observed frequencies.
  Example: Guess E $\mapsto$ most frequent character, and so on.

Cryptanalysis of Substitute Cipher

Ciphertext:
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJNDIFEFMDZCDM
QZKCEYFCJMYRNCWJCSZREXCHZUNMXZNZUCDRJXYYSMRTMEYIFZWDYVZ
VYFZUMRZCRWNZDZJJXZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR

- Tabulate the frequency distribution of characters:
  A appeared 0 times, B appeared 1 times, and so on
- Compare them with the known frequencies of English text.
- Guess parts of the mapping based on the observed frequencies.
  Example: Guess E $\mapsto$ most frequent character, and so on.
- **Note:** Some of the guesses may be wrong.

Cryptanalysis of Substitute Cipher

Ciphertext:
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJNDIFEFMDZCDM
QZKCEYFCJMYRNCWJCSZREXCHZUNMXZNZUCDRJXYYSMRTMEYIFZWDYVZ
VYFZUMRZCRWNZDZJJXZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR

- Tabulate the frequency distribution of characters:
  A appeared 0 times, B appeared 1 times, and so on
- Compare them with the known frequencies of English text.
- Guess parts of the mapping based on the observed frequencies.
  Example: Guess E $\mapsto$ most frequent character, and so on.
- **Note:** Some of the guesses may be wrong.
- But enough of the guesses will be correct to enable relatively quick decryption.
- For quick decryption use other knowledge of English.
  - u generally follows q.
  - h is likely to appear between t and e.
  - The frequencies of *digrams* and *trigrams*.
  - ...

Empirical distribution

Letter	Frequency	Letter	Frequency
A	0	N	9
B	1	O	0
C	15	P	1
D	13	Q	4
E	7	R	10
F	11	S	3
G	1	T	2
H	4	U	5
I	5	V	5
J	11	W	8
K	1	X	6
L	0	Y	10
M	16	Z	20

Cryptanalysis of Substitute Cipher

Empirical distribution

Letter	Frequency	Letter	Frequency
A	0	N	9
B	1	O	0
C	15	P	1
D	13	Q	4
E	7	R	10
F	11	S	3
G	1	T	2
H	4	U	5
I	5	V	5
J	11	W	8
K	1	X	6
L	0	Y	10
M	16	Z	20

- Most frequencies (≥ 10).

Z - 20;	D - 13
M - 16;	F, J - 11
C - 15;	R, Y - 10

Initial guess: Let $\mathcal{E}(k, \mathrm{E}) = Z$.

- We might expect that

  C, D, F, J, M, R, Y (frequency $\geq$ 10 each)

  are encryptions of (a subset of)

  T, A, O, I, N, S, H, R.

Initial guess: Let $\mathcal{E}(k, \mathrm{E}) = Z$.

- We might expect that

  $$\text{C, D, F, J, M, R, Y (frequency} \geq 10 \text{ each)}$$

  are encryptions of (a subset of)

  $$\text{T, A, O, I, N, S, H, R.}$$

- But these frequencies really do not vary enough to tell us what the correspondence might be.

Initial guess: Let $\mathcal{E}(k, \mathrm{E}) = Z$.

- So look at diagrams of the form _Z or Z_.
- DZ and ZW: 4 times each.
  NZ and ZU: 3 times each.
  RZ, HZ, XZ, FZ, ZR, ZV, ZC, ZD and ZJ: Twice each.

Initial guess: Let $\mathcal{E}(k, \mathrm{E}) = Z$.

- So look at diagrams of the form _Z or Z_.
- DZ and ZW: 4 times each.
  NZ and ZU: 3 times each.
  RZ, HZ, XZ, FZ, ZR, ZV, ZC, ZD and ZJ: Twice each.
- Observations 1:
  - ZW occurs 4 times, WZ occurs 0 times.
  - W occurs less often than many other characters.
  - Subsequent guesses: $\mathcal{E}(k, \mathrm{D}) = W$.

Cryptanalysis of Substitute Cipher

Initial guess: Let $\mathcal{E}(k, \mathrm{E}) = Z$.

- So look at diagrams of the form _Z or Z_.
- DZ and ZW: 4 times each.
  NZ and ZU: 3 times each.
  RZ, HZ, XZ, FZ, ZR, ZV, ZC, ZD and ZJ: Twice each.
- Observations 1:
  - ZW occurs 4 times, WZ occurs 0 times.
  - W occurs less often than many other characters.
  - Subsequent guesses: $\mathcal{E}(k, \mathrm{D}) = W$.
- Observations 2:
  - DZ occurs 4 times, ZD occurs 2 times.
  - With high probability, $\mathcal{D}(k, D) \in \{R, S, T\}$.
  - But it is not clear which of these 3 possibility is the correct one.

Guess: Let $\mathcal{E}(k, \mathrm{E}) = Z, \mathcal{E}(k, \mathrm{D}) = W$.

- Observations 3:
  - ZRW occurs near the beginning of the ciphertext, and RW occurs again later on.
  - Since R occurs frequently in the ciphertext and ND is a common digram.
  - Subsequent guesses:

$$\mathcal{E}(k, \mathrm{N}) = R.$$

Guess: Let $\mathcal{E}(k,\mathrm{E}) = Z, \mathcal{E}(k,\mathrm{D}) = W$.

- Observations 3:
  - ZRW occurs near the beginning of the ciphertext, and RW occurs again later on.
  - Since R occurs frequently in the ciphertext and ND is a common digram.
  - Subsequent guesses:

$$\mathcal{E}(k,\mathrm{N}) = R.$$

Partial Decryption:

- - - - - - -END - - - - - - - - - - - E - - - - -NED - - - - E -E - - - -
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJNDIFEFMDZCDM
- E - - - - - - - - - - - N - - D - - -EN - - - - E - - - - - E - E - - - N - - - - - - - N - - - - - - - ED - - – E
QZKCEYFCJMYRNCWJCSZREXCHZUNMXZNZUCDRJXYYSMRTMEYIFZWDYVZ
- – - E – - NE -ND - E - E - - ED - - - - - - N - - - - - - – - - - - - - - E - - - - ED - - - - - - - - D - -
VYFZUMRZCRWNZDZJJXZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJ
- E - -N
NZDIR

Guess: Let $\mathcal{E}(k,\mathrm{E}) = Z, \mathcal{E}(k,\mathrm{D}) = W, \mathcal{E}(k,\mathrm{N}) = R.$

- Observations 4:
  - NZ is a common diagram and ZN is not.
  - Subsequent guesses:

$$\mathcal{E}(k,\mathrm{H}) = N.$$

Guess: Let $\mathcal{E}(k,\mathrm{E}) = Z, \mathcal{E}(k,\mathrm{D}) = W, \mathcal{E}(k,\mathrm{N}) = R.$

- Observations 4:
  - NZ is a common diagram and ZN is not.
  - Subsequent guesses:

$$\mathcal{E}(k,\mathrm{H}) = N.$$

Further Decryption:

- - - - - - -END - - - - - - - - - - - E - - - - -NEDH - - -E - - - - - - - - - - - - - H - - - - - - - E - - - -
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJNDIFEFMDZCDM
- E - - - - - - - - - - - NH- -D - - EN - - - - E - H- - - EHE - - - N - - - - - - N - - - - - - ED - - - -E
QZKCEYFCJMYRNCWJCSZREXCHZUNMXZNZUCDRJXYYSMRTMEYIFZWDYVZ
- – - E – - NE - NDHE - E - - ED - - - - - - NH - - - -H - - - - - - - E - - - -ED - - - - - - - D - -
VYFZUMRZCRWNZDZJJXZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJ
HE - -N
NZDIR

Guess: Let $\mathcal{E}(k, \mathrm{E}) = Z, \mathcal{E}(k, \mathrm{D}) = W, \mathcal{E}(k, \mathrm{N}) = R, \mathcal{E}(k, \mathrm{H}) = N$.

- Observations 5:
  - AND is a very common trigram.
  - Subsequent guesses: (from the segment NE - NDHE suggests)

$$\mathcal{E}(k, \mathrm{A}) = C.$$

Guess: Let $\mathcal{E}(k, \mathrm{E}) = Z, \mathcal{E}(k, \mathrm{D}) = W, \mathcal{E}(k, \mathrm{N}) = R, \mathcal{E}(k, \mathrm{H}) = N.$

- Observations 5:
  - AND is a very common trigram.
  - Subsequent guesses: (from the segment NE - NDHE suggests)

$$\mathcal{E}(k, \mathrm{A}) = C.$$

Further Decryption:

- - - - - - -END - - - - - - - - - - - E - - - - -NEDH - - -E - - - - - - - - - - - - - - H - - - - - - - - E - - - -
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJNDIFEFMDZCDM
- E - - - - - - - - - - - NH- -D - - EN - - - - E - H- - - EHE - - - N - - - - - - - N - - - - - - - ED - - - -E
QZKCEYFCJMYRNCWJCSZREXCHZUNMXZNZUCDRJXYYSMRTMEYIFZWDYVZ
- – - E – - NE - NDHE - E - - ED - - - - - - - NH - - - -H - - - - - - - - E - - - -ED - - - - - - - - D - -
VYFZUMRZCRWNZDZJJXZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJ
HE - -N
NZDIR

Guess: Let $\mathcal{E}(k,\mathrm{E}) = Z, \mathcal{E}(k,\mathrm{D}) = W, \mathcal{E}(k,\mathrm{N}) = R, \mathcal{E}(k,\mathrm{H}) = N, \mathcal{E}(k,\mathrm{A}) = C.$

Further Decryption:

- - - - - - -END - - - - - -A - - - E -A - - NEDH - - -E - - - - - - A - - - - - - H - - - - - - -EA - - -
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJNDIFEFMDZCDM
- E - A - - - A - - -NHAD -A-EN - - A -E - H- - - EHE -A - N - - - - - - N - - - - - - ED - - - E
QZKCEYFCJMYRNCWJCSZREXCHZUNMXZNZUCDRJXYYSMRTMEYIFZWDYVZ
- – - E – - NEANDHE - E - - ED - -A - - - NH - - - -HA - - - A - E - - - -ED - - - - -A -D - -
VYFZUMRZCRWNZDZJJXZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJ
HE - -N

NZDIR

Guess: Let $\mathcal{E}(k, \text{E}) = Z, \mathcal{E}(k, \text{D}) = W, \mathcal{E}(k, \text{N}) = R, \mathcal{E}(k, (\text{H}) = N, \mathcal{E}(k, \text{A}) = C$

- Observations 6: Consider M
  - Second most common ciphertext character.
  - Partial decryption of $\mathcal{D}(k, \text{RNM}) = \text{NH}-$, suggests that H- is the beginning of a word.
  - So M probably encrypts a vowel.

Guess: Let $\mathcal{E}(k, \mathrm{E}) = Z, \mathcal{E}(k, \mathrm{D}) = W, \mathcal{E}(k, \mathrm{N}) = R, \mathcal{E}(k, (\mathrm{H}) = N, \mathcal{E}(k, \mathrm{A}) = C$

- Observations 6: Consider M
    - Second most common ciphertext character.
    - Partial decryption of $\mathcal{D}(k, \mathrm{RNM}) = \mathrm{NH}-$, suggests that H- is the beginning of a word.
    - So M probably encrypts a vowel.
    - A and E are already accounted, then

$$\mathcal{D}(k, \mathrm{M}) = \mathrm{I} \text{ or } \mathrm{O}.$$

    - “AI” is a much more likely digram than “AO”
    - Subsequent guesses: (from the digram CM)

$$\mathcal{E}(k, \mathrm{I}) = \mathrm{M}.$$

Guess: Let
$\mathcal{E}(k,\mathrm{E}) = Z, \mathcal{E}(k,\mathrm{D}) = W, \mathcal{E}(k,\mathrm{N}) = R, \mathcal{E}(k,\mathrm{H}) = N, \mathcal{E}(k,\mathrm{A}) = C, \mathcal{E}(k,\mathrm{I}) = \mathrm{M}.$

Further Decryption:

- - - - - -IEND - - - - - - - A - I - E -A - INE D H I - E - - - - - - - A - - - - I -H - - - - - I - EA - -I
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJNDIFEFMDZCDM
- E - A - - - A -I- -NHAD -A-EN - - A -E - H I - EHE -A - N - - - - - I N - I - - - - ED - - – E
QZKCEYFCJMYRNCWJCSZREXCHZUNMXZNZUCDRJXYYSMRTMEYIFZWDYVZ
- – - E – I NEANDHE - E - - ED - -A - - I NH I - - -HA I - - A - E -I- - -ED - - - - - -A -D - -
VYFZUMRZCRWNZDZJJXZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJ
HE - -N
NZDIR

Guess: Let
$\mathcal{E}(k,\mathrm{E}) = Z, \mathcal{E}(k,\mathrm{D}) = W, \mathcal{E}(k,\mathrm{N}) = R, \mathcal{E}(k,\mathrm{H}) = N, \mathcal{E}(k,\mathrm{A}) = C, \mathcal{E}(k,\mathrm{I}) = \mathrm{M}$.

- O is a common plaintext character.
- Guess $\mathcal{E}(k,O) \in \{D,F,J,Y\}$.
- Y seems to be the most likely possibility.
- Otherwise,

$$\begin{aligned} \mathcal{D}(k,\mathrm{CFM}) &= \mathrm{AOI}; \quad \text{if } \mathcal{E}(k,\mathrm{O}) = \mathrm{F} \text{ or} \\ \mathcal{D}(k,\mathrm{CJM}) &= \mathrm{AOI}; \quad \text{if } \mathcal{E}(k,\mathrm{O}) = \mathrm{J}, \end{aligned}$$

  giving long strings of vowels in both cases.
- Hence, assume $\mathcal{E}(k,\mathrm{O}) = \mathrm{Y}$.

Guess: Let $\mathcal{E}(k,\mathrm{E}) = Z, \mathcal{E}(k,\mathrm{D}) = W, \mathcal{E}(k,\mathrm{N}) = R, \mathcal{E}(k,\mathrm{H}) = N, \mathcal{E}(k,\mathrm{A}) = C, \mathcal{E}(k,\mathrm{I}) = \mathrm{M}, \mathcal{E}(k,\mathrm{O}) = \mathrm{Y}$.

- **Three most frequent ciphertext letters remaining:** D, F, J.
- **Conjecture:** $\{\mathrm{D},\mathrm{F},\mathrm{J}\} = \{\mathrm{r},\mathrm{s},\mathrm{t}\}$.
- Two occurrences of the trigram NMD suggest that

$$\mathcal{D}(k,\mathrm{D}) = \mathrm{S} \Rightarrow \mathcal{D}(k,\mathrm{NMD}) = \mathrm{HIS}.$$

- $\mathcal{D}(k,\mathrm{HNCMF}) = -\mathrm{HAI}-$ could be a decryption of CHAIR.
- Then let $\mathcal{D}(k,\mathrm{F}) = \mathrm{R}$ and $\mathcal{D}(k,\mathrm{H}) = \mathrm{C}$, which implies

$$\mathcal{D}(k,\mathrm{J}) = T \quad \text{[By process of elimination].}$$

Guess: Let $\mathcal{E}(k,\mathrm{E}) = Z, \mathcal{E}(k,\mathrm{D}) = W, \mathcal{E}(k,\mathrm{N}) = R, \mathcal{E}(k,\mathrm{H}) = N, \mathcal{E}(k,\mathrm{A}) = C, \mathcal{E}(k,\mathrm{I}) = \mathrm{M}, \mathcal{E}(k,\mathrm{O}) = \mathrm{Y}, \mathcal{E}(k,\mathrm{R}) = \mathrm{F}, \mathcal{E}(k,\mathrm{C}) = \mathrm{H}, \mathcal{E}(k,\mathrm{T}) = J.$

Further Decryption:

O-R -R IEND – RO - -ARI SE - A - I NE D H I S E - -T - - - ASS - -ITHS -R-R I SE AS I
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJNDIFEFMDZCDM
- E - A -ORATIONHA DTA-EN - - ACE - H I - EHE - ASNT- OO - I N - I - O- REDSO - E
QZKCEYFCJMYRNCWJCSZREXCHZUNMXZNZUCDRJXYYSMRTMEYIFZWDYVZ
- ORE – I NEANDHESETT- ED - -AC - I NH I SCHA I - - ACET I- -TED- -TO -ARDST
VYFZUMRZCRWNZDZJJXZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJ
HES -N

NZDIR

Partially Decrypted Text

Further Decryption:

O-R -R IEND – RO - -ARI SE - A - I NE D H I S E - -T - - - ASS - -ITHS -R-R I SE AS I
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJNDIFEFMDZCDM
- E - A -ORATIONHA DTA-EN - - ACE - H I - EHE - ASNT- OO - I N - I - O- REDSO - E
QZKCEYFCJMYRNCWJCSZREXCHZUNMXZNZUCDRJXYYSMRTMEYIFZWDYVZ
- ORE – I NEANDHESETT- ED - -AC - I NH I SCHA I - - ACET I- -TED- -TO -ARDST
VYFZUMRZCRWNZDZJJXZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJ
HES -N

NZDIR

Partially Decrypted Text

Further Decryption:

O-R -R IEND – RO - -ARI SE - A - I NE D H I S E - -T - - - ASS - -ITHS -R-R I SE AS I
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJNDIFEFMDZCDM
- E - A -ORATIONHA DTA-EN - - ACE - H I - EHE - ASNT- OO - I N - I - O- REDSO - E
QZKCEYFCJMYRNCWJCSZREXCHZUNMXZNZUCDRJXYYSMRTMEYIFZWDYVZ
- ORE – I NEANDHESETT- ED - -AC - I NH I SCHA I - - ACET I- -TED- -TO -ARDST
VYFZUMRZCRWNZDZJJXZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJ
HES -N

NZDIR

Plaintext

Our friend from Paris examined his empty glass with surprise, as if evaporation had taken place while he wasn't looking. I poured some more wine and he settled back in his chair, face tilted up towards the sun.

Partially Decrypted Text

Further Decryption:

O-R -R IEND – RO - -ARI SE - A - I NE D H I S E - -T - - - ASS - -ITHS -R-R I SE AS I
YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJNDIFEFMDZCDM
- E - A -ORATIONHA DTA-EN - - ACE - H I - EHE - ASNT- OO - I N - I - O- REDSO - E
QZKCEYFCJMYRNCWJCSZREXCHZUNMXZNZUCDRJXYYSMRTMEYIFZWDYVZ
- ORE – I NEANDHESETT- ED - -AC - I NH I SCHA I - - ACET I- -TED- -TO -ARDST
VYFZUMRZCRWNZDZJJXZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJ
HES -N
NZDIR

Plaintext

Our friend from Paris examined his empty glass with surprise, as if evaporation had taken place while he wasn't looking. I poured some more wine and he settled back in his chair, face tilted up towards the sun.

Conclusion

Although the mono-alphabetic substitution cipher has a large key space, it is still *insecure*.

Vigener Cipher (16'th Century, Rome)

- This cipher is named after Blaise de Vigenere.
- Poly-Alphabetic cipher.

Vigener Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, Z\}$ (English Alphabet).

Vigener Cipher (16'th Century, Rome)

- This cipher is named after Blaise de Vigenere.
- Poly-Alphabetic cipher.

Vigener Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, Z\}$ (English Alphabet).
- $\mathcal{K} = \{\textsf{keywords} \mid n \in \mathbb{N}$ and $\textsf{keywords} \in \{A, B, C, \ldots, Z\}^n = \mathbb{Z}_{26}^n\}$.

Vigener Cipher (16'th Century, Rome)

- This cipher is named after Blaise de Vigenere.
- Poly-Alphabetic cipher.

Vigener Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \ldots, Z\}$ (English Alphabet).
- $\mathcal{K} = \{\textsf{keywords} \mid n \in \mathbb{N}$ and $\textsf{keywords} \in \{A, B, C, \ldots, Z\}^n = \mathbb{Z}_{26}^n\}$.
- $\mathcal{E}$: Let the key be a n character long keyword $k = k_0 k_1 \ldots k_{n-1}$. If the plaintext is $m = m_0 m_1 m_2 \ldots$, then we encrypt is as

$$c_i := \left(m_i + k_{i \pmod n}\right) \pmod{26},$$

and $c = c_0 c_1 c_2 \ldots$.

Vigener Cipher (16'th Century, Rome)

- This cipher is named after Blaise de Vigenere.
- Poly-Alphabetic cipher.

Vigener Cipher

- $\mathcal{P} = \mathcal{C} = \{A, B, C, \dots, Z\}$ (English Alphabet).
- $\mathcal{K} = \{\textsf{keywords} \mid n \in \mathbb{N} \text{ and } \textsf{keywords} \in \{A, B, C, \dots, Z\}^n = \mathbb{Z}_{26}^n\}$.
- $\mathcal{E}$: Let the key be a n character long keyword $k = k_0 k_1 \dots k_{n-1}$. If the plaintext is $m = m_0 m_1 m_2 \dots$, then we encrypt is as

$$c_i := \left(m_i + k_{i \pmod n}\right) \pmod{26},$$

  and $c = c_0 c_1 c_2 \dots$.
- $\mathcal{D}$: Let the key be a n character long keyword $k = k_0 k_1 \dots k_{n-1}$. If the ciphertext is $c = c_0 c_1 c_2 \dots$, then we decrypt is as

$$m_i := \left(c_i - k_{i \pmod n}\right) \pmod{26},$$

  and $m = m_0 m_1 m_2 \dots$.

Vigener Cipher (16'th Century, Rome)

Example

- Let $n = 6$ and Keyword is $k = \text{CIPHER}$.

Vigener Cipher (16'th Century, Rome)

Example

- Let $n = 6$ and Keyword is k = CIPHER.
- **Plaintext:** THISCRYPTOSYSTEMISNOTSECURE.

Vigener Cipher (16'th Century, Rome)

Example

- Let $n = 6$ and Keyword is $k =$ CIPHER.
- **Plaintext:** THISCRYPTOSYSTEMISNOTSECURE.

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

- **Ciphertext:** VPXZGIAXIVWPUBTTMJPWIZITWZT.

Cryptanalysis of Vigener Cipher

Let n is known

- Make the matrix from the ciphertext $c = c_0 c_1 c_2 \ldots$ as given below:

c_0	c_1	c_2	$\cdots$	c_{n-1}
c_n	c_{n+1}	c_{n+2}	$\cdots$	c_{2n-1}
c_{2n}	c_{2n+1}	c_{2n+2}	$\cdots$	c_{3n-1}
c_{3n}	c_{3n+1}	c_{3n+2}	$\cdots$	c_{3n-1}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Let n is known

- Make the matrix from the ciphertext $c = c_0 c_1 c_2 \ldots$ as given below:

c_0	c_1	c_2	$\cdots$	c_{n-1}
c_n	c_{n+1}	c_{n+2}	$\cdots$	c_{2n-1}
c_{2n}	c_{2n+1}	c_{2n+2}	$\cdots$	c_{3n-1}
c_{3n}	c_{3n+1}	c_{3n+2}	$\cdots$	c_{3n-1}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

- All the ciphertext symbols of each column of the above table are encrypted by a single character.
- Find the most frequent character of each column and it most likely the encryption of E.
- For each column, the difference between most frequent character and E is the part of the key.

Let n is unknown

- Repeat the above procedure for $n = 1, 2, 3, \ldots$, until the decryption makes sense.

Let n is unknown

- Repeat the above procedure for $n = 1, 2, 3, \ldots$, until the decryption makes sense.
- More improved version: Use Kasiski Test. (proposed by Friedrich Kasiski in 1863).
  - Charles Babbage discovered it in 1854.

Let n is unknown

- Repeat the above procedure for $n = 1, 2, 3, \ldots$, until the decryption makes sense.
- More improved version: Use Kasiski Test. (proposed by Friedrich Kasiski in 1863).
  - Charles Babbage discovered it in 1854.
- Further improvement: Use of Index of Coincidence by William Friedman in 1920.

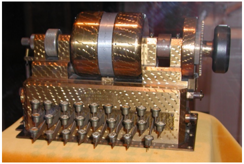


Figure: The Hebern machine (Single Rotor)

Rotor Machines (1870-1943)

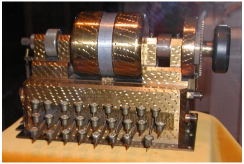


Figure: The Hebern machine (Single Rotor)

- Broken just using letter frequencies, diagrams and trigrams if sufficient ciphertexts are given.
- Key can be recovered.

Rotor Machines (1870-1943)

Figure: Most Famous Enigma (Three Rotor)

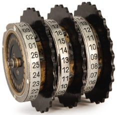


Figure: Example of Rotor

- Employed extensively by Nazi Germany during World War II.
- Was broken.
- **Alan Turing** was part of the team of those who broke Enigma.

Data Encryption Standard (1974)

- DES: 56 bit keys, 64-bit block size
- AES (2001)
- Salsa20 (2008) and so on.

Study At Home

- Affine cipher and its Cryptanalysis.
- Hill cipher and its Cryptanalysis.
- Permutation cipher and its Cryptanalysis.

End