

Glimpses of Cryptography MAC MATH FEST 2021

MD Karimulla Haque

Guided by, Dr. Nanda Das

June 27, 2021

Agenda Introduction

Basic Terminology

Caesar Cinhei

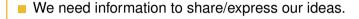
Example

Math behind this

Different type of

RSA

Choosing keys
Encryption
Decryption
Example





Agenda Introduction

Basic Terminology

Caesar Cipher

Example

Different type o

Ciphers

RSA

Choosing keys Encryption Decryption Example

References

■ We need information to share/express our ideas.

Some information are valuable. Hence we need protection.



Agenda Introduction

Basic Terminology

Caesar Ciphe

Example

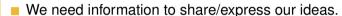
Math behind thi

Different type of

RSA

Choosing keys
Encryption
Decryption
Example

Poforoncos



- Some information are valuable. Hence we need protection.
- One of protection method is Cryptography.



Agenda

Basic Terminology

Caesar Ciphe

Example Math behind this

Different type o

Cipners

Choosing keys
Encryption
Decryption
Example
BSA Numbers

- We need information to share/express our ideas.
- Some information are valuable. Hence we need protection.
- One of protection method is Cryptography.
- Cryptography is used in ATM, Email-Password, E-Payment,
 E-Commerce, Electronic Voting, Defense Services, Securing Data,
 Access Control etc.



What is Cryptography?



Basic Terminology

Caesar Cinher

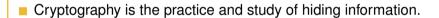
Example

math benind this

Different type of

RSA

Choosing keys Encryption Decryption Example





What is Cryptography?

Agenda Introduction

Basic Terminology

Caesar Ciphe

Example Math behind th

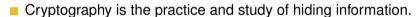
Different type of

Ciphers

RSA

Choosing keys Encryption Decryption Example

Poforoncoe



It is a branch of both Mathematics and Computer science.



Agenda

Basic Terminology

Caesar Cipher

Example

Math behind this

Different type of

RSA

Choosing keys
Encryption
Decryption
Example

References

■ Plaintext: original message



Agenda

Basic Terminology

Caesar Cipher

Example

math benind this

ifferent type of

RSA

Choosing keys
Encryption
Decryption
Example
RSA Numbers

References

Plaintext: original message

Ciphertext: coded message



Introduction

Basic Terminology

Basic Terminology

Caesar Cipher

Math behind this

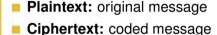
Different type of

Ciphers

Choosing ke

Encryption
Decryption
Example

Peteronce



Encipher (Encrypt): converting Plaintext to Ciphertext.



Agenda
Introduction
Basic Terminology

Caesar Cipher

Example Math behind this

Different type o

Ciphers

Choosing ke

Encryption
Decryption
Example



- Ciphertext: coded message
- Encipher (**Encrypt**): converting Plaintext to Ciphertext.
- Decipher (Decrypt): reconverting Ciphertext to Plaintext.



Agenda Introduction Basic Terminology

Caesar Cipher

Example Math behind this

Different type of

Ciphers

Choosing key

Encryption Decryption Example

HSA Numbers

Plaintext: original message

Ciphertext: coded message

Encipher (Encrypt): converting Plaintext to Ciphertext.

Decipher (Decrypt): reconverting Ciphertext to Plaintext.

Cipher: algorithm for performing Encryption or Decryption.



Agenda Introduction Basic Terminology

Caesar Cipher

Example Math behind this

Different type o

RSΔ

Choosing keys
Encryption
Decryption
Example

Example RSA Numbers

References

Plaintext: original message

Ciphertext: coded message

Encipher (Encrypt): converting Plaintext to Ciphertext.

Decipher (Decrypt): reconverting Ciphertext to Plaintext.

Cipher: algorithm for performing Encryption or Decryption.

Key: unique info used in cipher known only sender and receiver.



Caesar Cipher

Agenda
Introduction
Basic Terminology

Caesar Cipher

Example Math behind this

Different type of

RSA

Choosing keys Encryption Decryption Example RSA Numbers

References

 One of the earliest known example of substitution cipher.



Figure: Julius Caesar



Caesar Cipher

Agenda
Introduction
Basic Terminology

Caesar Cipher

Example Math behind this

Different type of

RSA

Choosing keys
Encryption
Decryption
Example
BSA Numbers

- One of the earliest known example of substitution cipher.
- Said to have been used by Julius Caesar to communicate with his army (secretly).



Figure: Julius Caesar



Caesar Cipher

Agenda
Introduction
Basic Terminology

Caesar Cipher

Example Math behind this

Different type of

RSA

Encryption
Decryption
Example
RSA Numbers

- One of the earliest known example of substitution cipher.
- Said to have been used by Julius Caesar to communicate with his army (secretly).
- Each character of a plaintext message is replaced by **n position down** in the alphabet.



Figure: Julius Caesar



Basic Terminology

Example

Math behind this

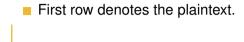




Figure: The earliest cipher equipment developed for substitution ciphers.



Agenda Introduction

Introduction Basic Terminology

Caesar Ciphe

Example

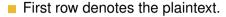
Math behind this

Different type of

RSA

Choosing keys Encryption Decryption Example RSA Numbers

Reference



Second row denotes the ciphertext.



Figure: The earliest cipher equipment developed for substitution ciphers.



Agenda
Introduction
Basic Terminology

Caesar Ciphe

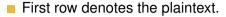
Example

Math behind this

Different type of

RSA

Choosing keys
Encryption
Decryption
Example
RSA Numbers



- Second row denotes the ciphertext.
- Ciphertext is obtain by shifting the original letter by n position to the right.



Figure: The earliest cipher equipment developed for substitution ciphers.



Agenda Introduction Basic Terminology

. .

Example

Math behind this

Different type of

RSA

Choosing keys
Encryption
Decryption
Example

- First row denotes the plaintext.Second row denotes the ciphertext.
- Ciphertext is obtain by shifting the original letter by n position to the right.
 - In this example, it is shifted by 3 to the right.
 - A becomes D
 - B becomes E
 - X becomes A
 - and so on · · ·

Α	В	С	 Х	Υ	Z
D	Е	F	 Α	В	С



Figure: The earliest cipher equipment developed for substitution ciphers.





Introduction Basic Terminology

Caesar Cipher

Example

Math behind this

Different type of

RSA

Choosing keys
Encryption
Decryption
Example

References



Suppose the following plaintext is to be encrypted ATTACK AT DAWN

Agenda Introduction Basic Terminology

Caesar Cipher

Example

Math behind this

Different type of

RSA

Encryption
Decryption
Example

References

Suppose the following plaintext is to be encrypted ATTACK AT DAWN

By shifting each letter by 3 to the right. The resulting ciphertext would be DWWDFN DW GDZQ

Α	В	С	 X	Υ	Z
D	Е	F	 Α	В	O



Agenda

Introduction
Basic Terminology

Caesar Cipher

Example

Math behind this

Different type of Ciphers

RSA

Choosing keys
Encryption
Decryption
Example

References



One could shift other than 3 letters apart.

Agenda Introduction

Basic Terminology

Caesar Ciphe

Example

Math behind this

Different type of Ciphers

RSA

Choosing keys
Encryption
Decryption
Example
BSA Numbers

References



One could shift other than 3 letters apart.

The offset (Number of shift) is called key.

Agenda
Introduction
Basic Terminology

Caesar Cinhe

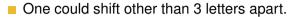
Example

Math behind this

Ciphers

RSA

Choosing keys Encryption Decryption Example RSA Numbers



- The offset (Number of shift) is called key.
- Decryption process:
 - Given that the key is known, just shift back n letter to the left.



Agenda
Introduction
Basic Terminology

Caesar Ciphe

Example

Math behind this

Ciphers

HSA

Encryption
Decryption
Example
RSA Numbers

References



One could shift other than 3 letters apart.

The offset (Number of shift) is called key.

Decryption process:

■ Given that the key is known, just shift back n letter to the left.

Example:

Ciphertext:

WJYZWS YT GFXJ

Key used: 5

Plaintext:

RETURN TO BASE

Α	В	С	 Χ	Υ	Ζ
V	W	Х	 S	Т	U

Agenda

Introduction Basic Terminology

Caesar Cipher

Math behind this

Different type of

RSA

Choosing keys
Encryption
Decryption
Example
RSA Numbers

References



Can be represented using modular arithmetic.

Agenda

Introduction Basic Terminology

Caesar Ciphe

Example

Math behind this

Ciphers

RSA

Choosing keys Encryption Decryption Example RSA Numbers

References



Can be represented using modular arithmetic.

- Assume that:
 - A = 0, B = 1, C = 2, ..., Y = 24, Z = 25

Agenda

Introduction Basic Terminology

Caesar Cipher

Example

Math behind this

Different type o Ciphers

RSA

Choosing keys
Encryption
Decryption
Example

References



- Can be represented using modular arithmetic.
- Assume that:

$$A = 0, B = 1, C = 2, ..., Y = 24, Z = 25$$

Encryption process can be represented as:

$$y = E(x) = (x + k) \pmod{26}$$

Agenda

Introduction Basic Terminolog

Caesar Ciphe

Math behind this

Matri beriind triis

Different type of Ciphers

RSA

Encryption
Decryption
Example
RSA Numbers

References

Can be represented using modular arithmetic.

Assume that:

$$A = 0, B = 1, C = 2, \dots, Y = 24, Z = 25$$

Encryption process can be represented as:

$$y = E(x) = (x + k) \pmod{26}$$

Decryption process can be represented as:

$$x = D(y) = (y - k) \pmod{26}$$

where

- \mathbf{x} is the plaintext
- y is the ciphertext
- k is the number of shift
- There are 26 letters in the alphabet (English alphabet).

Symmetric Ciphers

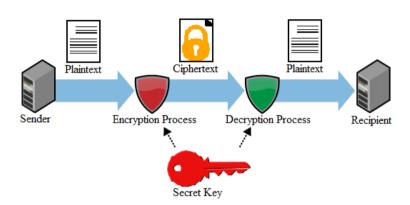
Basic Terminology

Math behind this

Different type of **Ciphers**

RSA Numbers





Asymmetric Ciphers

genda

Introduction Basic Terminology

Caesar Cipher

Example

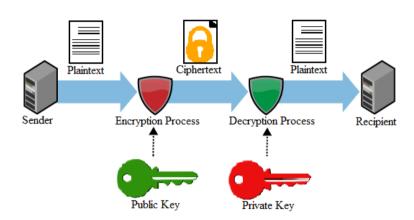
Math behind this

Different type of Ciphers

RSA

Choosing keys Encryption Decryption Example RSA Numbers





Agenda Introduction Basic Terminology

Caesar Cipher
Example
Math behind this

Different type of

Ciphers

HOA

Choosing keys
Encryption
Decryption
Example

References

The most common public-key algorithm is the RSA cryptography, named for its inventors (Rivest, Shamir and Adleman).



Figure: Inventers of RSA (Ronald L. Rivest, Adi Shamir and Leonard Adleman)



Agenda Introduction Basic Terminology

Caesar Cipher

Example Math behind this

Different type of Ciphers

ПОА

Encryption
Decryption
Example
RSA Numbers

- The most common public-key algorithm is the RSA cryptography, named for its inventors (Rivest, Shamir and Adleman).
- RSA do –
 Encryption/Decryption/Key
 Generation .



Figure: Inventers of RSA (Ronald L. Rivest, Adi Shamir and Leonard Adleman)



Agenda
Introduction
Basic Terminology

Caesar Cipher

Math behind this

Different type o Ciphers

пом

Encryption
Decryption
Example
RSA Numbers

- The most common public-key algorithm is the RSA cryptography, named for its inventors (Rivest, Shamir and Adleman).
- RSA do –
 Encryption/Decryption/Key
 Generation .
- Two types of keys



Figure: Inventers of RSA (Ronald L. Rivest, Adi Shamir and Leonard Adleman)



Agenda
Introduction
Basic Terminology

Caesar Cipher Example Math behind this

Different type o

HSA

Encryption
Decryption
Example
RSA Numbers

- The most common public-key algorithm is the RSA cryptography, named for its inventors (Rivest, Shamir and Adleman).
- RSA do –
 Encryption/Decryption/Key
 Generation .
- Two types of keys
 - Private key (to be kept confidential)



Figure: Inventers of RSA (Ronald L. Rivest, Adi Shamir and Leonard Adleman)



RSA

Basic Terminology

Math behind this

- The most common public-key algorithm is the RSA cryptography, named for its inventors (Rivest, Shamir and Adleman).
- RSA do -Encryption/Decryption/Key Generation.
- Two types of keys
 - Private key (to be kept confidential)
 - Public key (known to everyone)



Figure: Inventers of RSA (Ronald L. Rivest. Adi Shamir and Leonard Adleman)



genda

Introduction Basic Terminology

Caesar Cipher

Math behind this

Ciphers

RSA

Choosing keys

Encryption
Decryption

RSA Number

References



Choose two large prime numbers p, q (e.g., 1024 bits each)

genda

Introduction Basic Terminology

Caesar Cipher

Example

Math behind this

iferent type of

RSA

Choosing keys

Decryption Example RSA Numbers

References



Compute n = pq



genda

Introduction Basic Terminology

Caesar Ciphe

Example

Math behind this

Different type of

пом

Choosing keys

Decryption

RSA Number



- Compute n = pq
- $Z_n' = Z_{pq}'$ contains all integers in the range [1, pq) that are relatively prime to both p and q



Agenda

Introduction Basic Terminology

Caesar Ciphe

Example

Math behind this

Matir beriirid tris

Ciphers

noA

Choosing keys

Encryption

Example RSA Number

- Choose two large prime numbers p, q (e.g., 1024 bits each)
- Compute n = pq
- $Z_n' = Z_{pq}'$ contains all integers in the range [1, pq) that are relatively prime to both p and q
- Size of Z_n is $\phi(pq) = (p-1)(q-1) = z$ (say)



Basic Terminology

Math behind this

Choosing keys

Compute n = pq

 $Z_n' = Z_{nq}$ contains all integers in the range [1, pq) that are relatively prime to both p and q

Choose two large prime numbers p, q (e.g., 1024 bits each)

- Size of Z_n' is $\phi(pq) = (p-1)(q-1) = z$ (say)
- Choose e (with 1 < e < z) that has no common factors with z (i.e., e and z are relatively prime; gcd(e, z) = 1)



Agenda

Introduction Basic Terminology

Caesar Ciphe

Example
Math behind this

Different type of

Choosing keys

Encryption

Example RSA Number

- Choose two large prime numbers p, q (e.g., 1024 bits each)
- Compute n = pq
- $Z_n' = Z_{pq}'$ contains all integers in the range [1, pq) that are relatively prime to both p and q
- Size of Z_n' is $\phi(pq) = (p-1)(q-1) = z$ (say)
- Choose e (with 1 < e < z) that has no common factors with z (i.e., e and z are relatively prime; gcd(e, z) = 1)
- Choose **d** such that ed 1 is exactly divisible by z (i.e., $ed \mod z = 1$; ed = 1 + kz, k is an integer)



Agenda

Introduction Basic Terminology

Caesar Ciphe

Example Math behind this

Different type o

Choosing keys

Encryption
Decryption
Example

- Choose two large prime numbers p, q (e.g., 1024 bits each)
- Compute n = pq
- $Z_n' = Z_{pq}'$ contains all integers in the range [1, pq) that are relatively prime to both p and q
- Size of Z_n' is $\phi(pq) = (p-1)(q-1) = z$ (say)
- Choose e (with 1 < e < z) that has no common factors with z (i.e., e and z are relatively prime; gcd(e, z) = 1)
- Choose d such that ed 1 is exactly divisible by z (i.e., $ed \mod z = 1$; ed = 1 + kz, k is an integer)
- Public key is (n, e)



Agenda Introduction

Introduction
Basic Terminology

Caesar Ciphe

Example Math behind this

Different type of

Choosing k

Choosing keys

Example RSA Numbers

- Choose two large prime numbers p, q (e.g., 1024 bits each)
- Compute n = pq
- $Z_n' = Z_{pq}'$ contains all integers in the range [1, pq) that are relatively prime to both p and q
- Size of Z_n' is $\phi(pq) = (p-1)(q-1) = z$ (say)
- Choose e (with 1 < e < z) that has no common factors with z (i.e., e and z are relatively prime; gcd(e, z) = 1)
- Choose d such that ed 1 is exactly divisible by z (i.e., $ed \mod z = 1$; ed = 1 + kz, k is an integer)
- Public key is (n, e)
- Private key is d



Encryption

Basic Terminology

Math behind this

Encryption Decryption RSA Numbers





To encrypt plaintext,

Encryption

Basic Terminology

Math behind this

Encryption

To encrypt plaintext,

a given message M, where $M \in \mathbb{Z}_n - \{0\}$, 0 < M < n



Encryption

Introduction

Introduction Basic Terminology

Caesar Cipher

Example Math behind this

Different type of

Choosing ke

Encryption
Decryption
Example

- To encrypt plaintext,
- a given message M, where $M \in \mathbb{Z}_n \{0\}$, 0 < M < n
- Ompute $C = M^e \mod n$
 - (i.e., remainder when M^e is divided by n)



Decryption

Basic Terminology

Math behind this

Decryption

To decrypt received ciphertext,



June 27, 2021

Decryption

Basic Terminology

Decryption

- To decrypt received ciphertext,
- a given message C, where $C \in \mathbb{Z}_n \{0\}$



Decryption

Introduction
Basic Terminology

Caesar Cipher

Example Math behind this

Different type of

HSA

Choosing key Encryption

Decryption

RSA Number

- To decrypt received ciphertext,
- lacksquare a given message C, where $C \in \mathbb{Z}_n \{0\}$
- Compute $M = C^d \mod n$
 - (i.e., remainder when C^d is divided by n)



Basic Terminology

Math behind this

Example



Receiver choose p = 5, q = 7. Then n = 35, z = 24

Agenda

Introduction
Basic Terminology

Caesar Cipher

Example
Math behind thi

Different type of

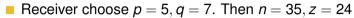
RSA

Choosing keys Encryption Decryption

Example

RSA Numbers

References



e = 5 (so that *e* and *z* are relatively prime)



Agenda

Introduction Basic Terminology

Caesar Ciphei

Example Math behind this

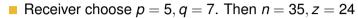
Different type of

RSA

Choosing key Encryption Decryption

Example

RSA Numbers



- e = 5 (so that e and z are relatively prime)
- d = 29 (so that *ed*1 exactly divisible by *z*)



Agenda

Introduction Basic Terminology

Caesar Ciphe

Example Math behind this

Different type of

DCA.

Choosing key Encryption

Example

RSA Number

- Receiver choose p = 5, q = 7. Then n = 35, z = 24
- e = 5 (so that e and z are relatively prime)
- d = 29 (so that *ed*1 exactly divisible by z)
- encrypt:

letter	m	m ^e	$c = m^e \mod n$	
I	12	1524832	17	



Agenda

Introduction Basic Terminology

Caesar Ciphe

Example

Math behind this

Different type of

RSA

Choosing key Encryption Decryption

Example

RSA Numbers

References

- Receiver choose p = 5, q = 7. Then n = 35, z = 24
- e = 5 (so that e and z are relatively prime)
- d = 29 (so that *ed*1 exactly divisible by z)
- encrypt:

letter	m	m ^e	$c = m^e \mod n$	
I	12	1524832	17	

decrypt:

	С	c^d	$m = c^d \mod n$	letter
Ì	17	481968572106750915091411825223071697	12	I



Agenda
Introduction
Basic Terminology

Caesar Cipher

Math behind this

Ciphers

HSA

Encryption
Decryption

Example

Poforoncos

The number of bits for n should be at least 1024. This means that n should be around 2¹⁰²⁴ or, 309 decimal digits.



Agenda
Introduction
Basic Terminology

Caesar Cipher

Example Math behind this

Different type of

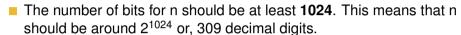
RSA

Choosing key Encryption Decryption

Example

RSA Numbers

References



■ The two primes p and q must each be at least **512 bits**.



Agenda Introduction Basic Terminology

Caesar Cipher Example Math behind this

Different type of

Ciphers

Choosing ke

Encryption
Decryption

Example BSA Numbers

RSA Numbers



- The number of bits for n should be at least **1024**. This means that n should be around 2¹⁰²⁴ or, 309 decimal digits.
- The two primes p and q must each be at least **512 bits**.
- The values of *p* and *q* should **not** be very close to each other.

Agenda
Introduction
Basic Terminology

Caesar Cipher

Math behind this

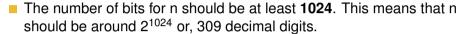
Different type of Ciphers

Choosin

Choosing key Encryption Decryption

Example BSA Numbers

RSA Numbers



- The two primes p and q must each be at least 512 bits.
- The values of *p* and *q* should **not** be very close to each other.
- Both p-1 and q-1 should have at least one large prime factor.



Agenda Introduction Basic Terminology

Caesar Cipher

Different type o

Ciphers

Choosing

Encryption
Decryption

Example BSA Number

RSA Numbers

- The number of bits for n should be at least 1024. This means that n should be around 2¹⁰²⁴ or, 309 decimal digits.
- The two primes p and q must each be at least **512 bits**.
- The values of p and q should **not** be very close to each other.
- Both p-1 and q-1 should have at least one large prime factor.
- The ratio $\frac{p}{q}$ should not be close to a rational number with a small enumerator and denominator.



Agenda Introduction Basic Terminology

Caesar Cipher Example

Different type of

Ciphers

Chassi

Choosing key Encryption Decryption

Example BSA Number

RSA Numbers

- The number of bits for n should be at least 1024. This means that n should be around 2¹⁰²⁴ or, 309 decimal digits.
- The two primes p and q must each be at least **512 bits**.
- The values of *p* and *q* should **not** be very close to each other.
- Both p-1 and q-1 should have at least one large prime factor.
- The ratio $\frac{p}{q}$ should not be close to a rational number with a small enumerator and denominator.
- The modulus *n* must not be shared.



Agenda
Introduction
Basic Terminology

Caesar Cipher

Example
Math behind this

Different type of

RSA

Choosing keys
Encryption
Decryption
Example

RSA Numbers

References

RSA numbers are a collection of large semiprimes published by RSA Laboratories to encourage research in integer factorization.



Agenda Introduction Basic Terminology

Caesar Cipher

Math behind this

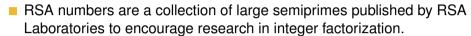
Different type of

RSA

Choosing keys
Encryption
Decryption
Example

RSA Numbers

References



RSA-768 (with 768 bits, 232 decimal digits) was factored in December 2009 after about 2,000 core-years of computation.



Agenda Introduction Basic Terminology

Caesar Cipher

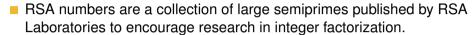
Math behind this

Ciphers

HOA

Choosing keys
Encryption
Decryption
Example
RSA Numbers

Peteronce



- RSA-768 (with 768 bits, 232 decimal digits) was factored in December 2009 after about 2,000 core-years of computation.
- RSA-1024 (with 1024 bits, 309 decimal digits) remains unbroken and is still considered secure for many applications.



Agenda Introduction Basic Terminology

Caesar Cipher Example Math behind this

Different type o

DCA

Choosing keys Encryption Decryption Example

RSA Numbers

RSA numbers are a collection of large semiprimes published by RSA Laboratories to encourage research in integer factorization.

- RSA-768 (with 768 bits, 232 decimal digits) was factored in December 2009 after about 2,000 core-years of computation.
- RSA-1024 (with 1024 bits, 309 decimal digits) remains unbroken and is still considered secure for many applications.
- RSA-2048 has 617 decimal digits (2048 bits). It is the largest of the RSA numbers and carried the largest cash prize for its factorization, \$200,000.



Basic Terminology

Math behind this

RSA Numbers

- RSA numbers are a collection of large semiprimes published by RSA Laboratories to encourage research in integer factorization.
- RSA-768 (with 768 bits, 232 decimal digits) was factored in December 2009 after about 2,000 core-years of computation.
- RSA-1024 (with 1024 bits, 309 decimal digits) remains unbroken and is still considered secure for many applications.
- RSA-2048 has 617 decimal digits (2048 bits). It is the largest of the RSA numbers and carried the largest cash prize for its factorization, \$200,000.
- As of today, no RSA number larger than 768 bits has been successfully factored, highlighting the strength of modern public-key cryptography.



References

Agenda
Introduction
Basic Terminology

Caesar Cipher

Example Math behind this

Different type o

пом

Encryption
Decryption
Example
RSA Numbers

- Yan, S. Y. Cryptanalytic Attacks on RSA. Springer, 2008.
- Delfs, H. and Knebl, H. Introduction to Cryptography: Principles and Applications. Springer, 3rd Edition, 2015.
- Stinson, D. R. Cryptography: Theory and Practice. Chapman Hall/CRC, 4th Edition, 2018.
- Lecture video (Bengali) is available at: https://youtu.be/XRfuKKCQVBA?t=1460
- Pictures were taken from Google Images.



Thank You

