MATHEMATICAL CIPHERS

Delving into the Cryptographic Complexities of
Number Theory and Abstract Algebra

MENTORS

Naman Gupta
namangupta22@iitk.ac.in, 7678600231

Ishan Dandwani
ishand22@iitk.ac.in, 9887541586

Sanskar Yaduka
sanskary22@iitk.ac.in, 8434842395

WEEK 1-3

- Discover key Number Theory concepts like Euclid’s Algorithm and Fermat’s Little Theorem.
- Explore practical applications such as Euler’s Totient Function and the Chinese Remainder Theorem.
- Delve deeper into advanced topics like Algebraic Number Theory and Combinatorial Number Theory.
- Gain a comprehensive understanding of essential concepts such as Divisibility and Density in Number Theory.
- Conclude with an interactive week dedicated to brainstorming problems and engaging in assignment tasks.

WEEK 4-6

- Our exploration will commence with delving into group theory, recognizing its foundational importance.
- Groups will be introduced, with a focus on their abstract nature and their significance across diverse applications emphasis will be placed on the relevance of groups, particularly in cryptographic algorithms.
- We'll explore rings and fields, highlighting their resilience and importance in key exchange algorithms and hashing.
- We'll delve into a comprehensive examination of various problems to reinforce understanding and foster a broader approach to problem-solving within these mathematical frameworks.

WEEK 7-10

- Cryptographic Protocols: Explore RSA, Diffie-Hellman, ECC, and AES, focusing on their design and application in cryptography.
- Security Analysis: Investigate algorithm security, covering computational hardness, key sizes, and vulnerabilities like brute force attacks.
- Practical Implementations: Examine real-world applications such as secure messaging, digital signatures, and secure computation.
- Recent Advances: Survey post-quantum cryptography, homomorphic encryption, and zero-knowledge proofs, highlighting their significance.
- Future Directions: Discuss evolving challenges and potential paths forward in cryptography.

LOGISTICS FOR THE PROJECT

PROJECT DURATION 8-10 WEEKS

WEEKLY COMMITMENT 7-8 HRS

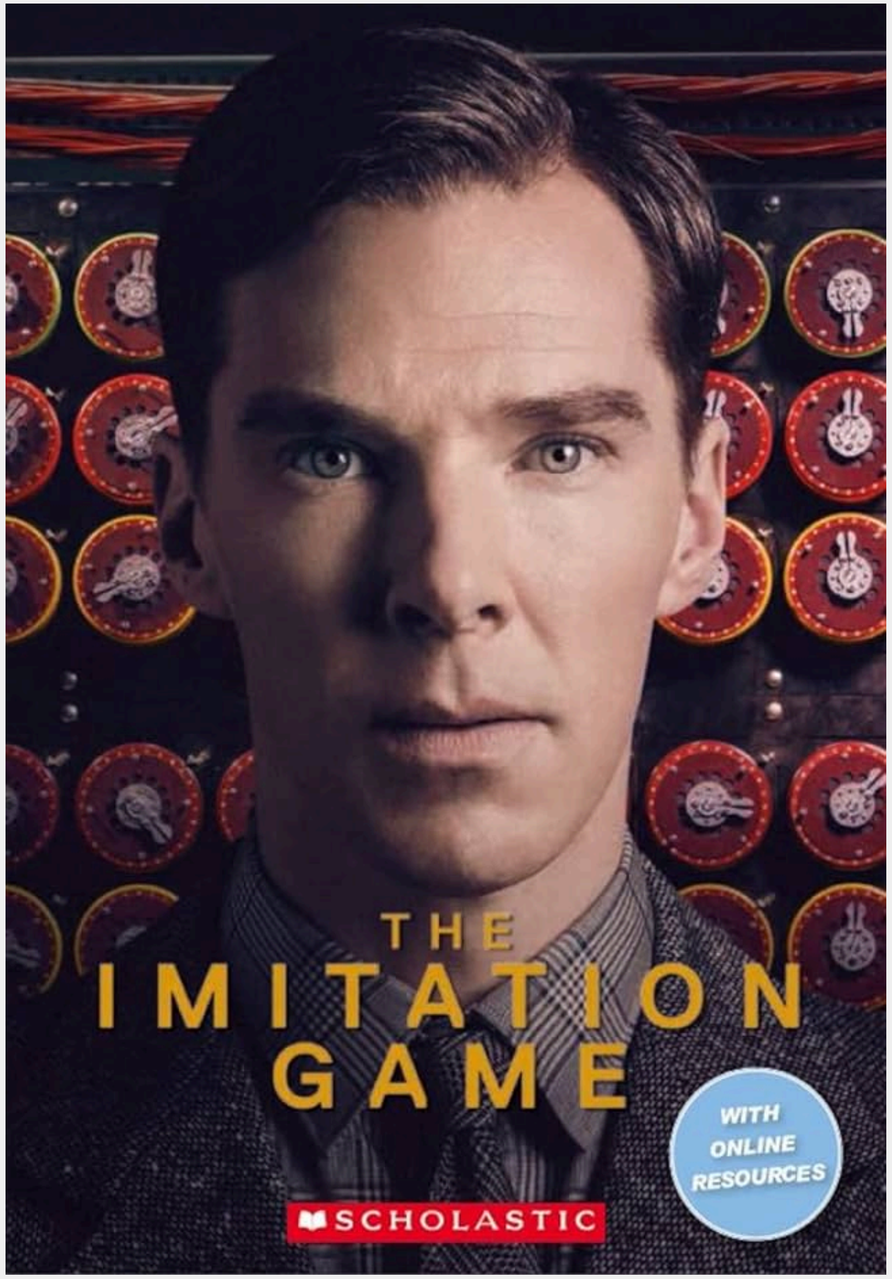
PREREQS - BASIC MATH APTITUDE

BIWEEKLY ASSIGNMENTS

EXPECTED NUMBER OF MENTEES - 50 (Y23S, Y22S)

Let’s begin!


THE TRUE ENIGMA
WAS THE MAN WHO CRACKED
THE CODE
BENEDICT CUMBERBATCH
KEIRA KNIGHTLEY
THE IMITATION GAME
COMING SOON
STUDIOCANAL


THE
IMITATION
GAME
WITH
ONLINE
RESOURCES
SCHOLASTIC

The Imitation Game

IMDb

During World War II, the English mathematical genius **Alan Turing** tries to crack the German Enigma code with help from fellow mathematicians while attempting to come to terms with his troubled private life.

Enigma was an electromechanical cipher machine used by the German military to encrypt their messages. It was considered unbreakable due to its complex encryption mechanism and the sheer number of possible settings. However, Turing, along with other codebreakers at Bletchley Park, developed the Bombe, an electromechanical device that helped decipher Enigma-encoded messages.

Turing Test

- Proposed by Alan Turing in 1950, it is a way to measure a machine's ability to exhibit intelligent behavior equivalent to, or indistinguishable from, that of a human.

- The test involves a human evaluator interacting with both a machine and another human through a text-based interface (such as a chat), without knowing which is which. If the evaluator cannot reliably distinguish the machine from the human based on the conversation, then the machine is said to have passed the Turing Test.

(Its a method to check for efficient ML and AI models.
Not related to Cryptography though!)

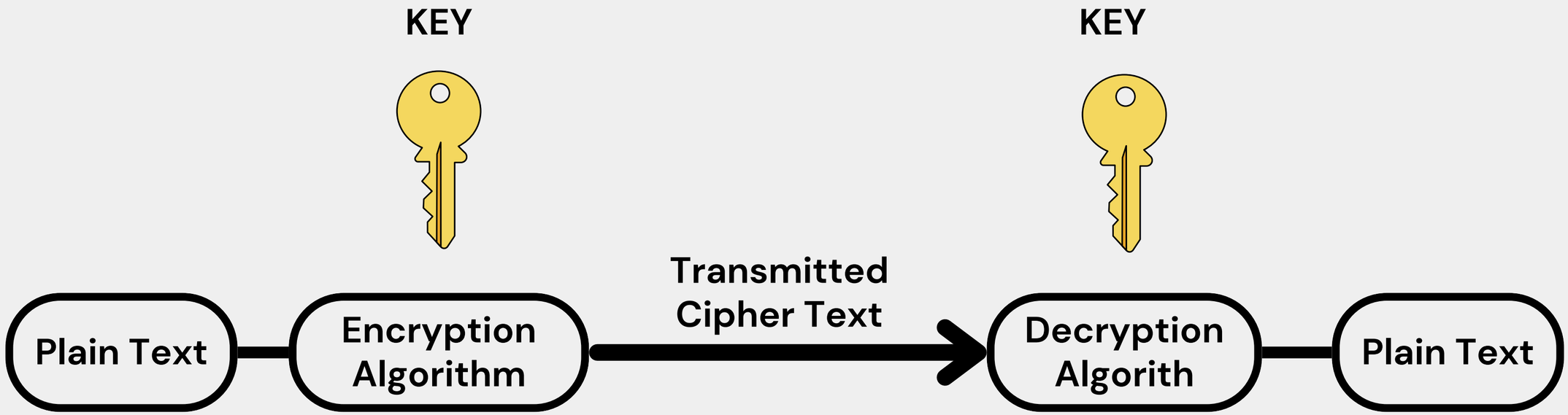
So finally...

What is Cryptography?

The art or science encompassing the principles and methods of transforming inteligible into one that is intelligible, and then retransforming that into its original form.

So finally...

What is Cryptography?

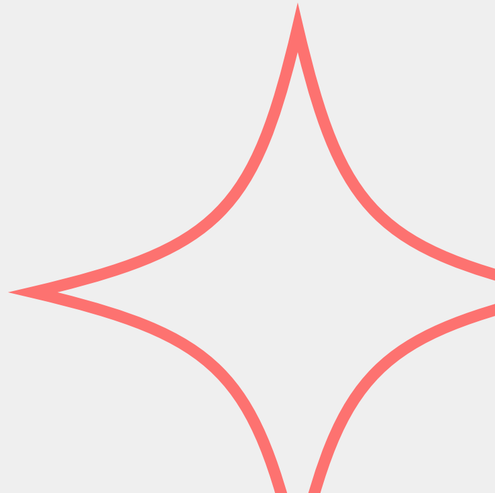


Private Key Encryption v/s Public Key Encryption

- In **private key encryption**, also known as symmetric encryption, the **same key is used for both encryption and decryption**. The parties involved must share the private key securely beforehand.

- In **public key encryption**, also known as asymmetric encryption, two keys are used: **a public key for encryption and a private key for decryption**. Public key encryption enables secure communication between parties without needing to share a secret key beforehand.

- **Private key encryption is faster and more efficient but requires securely sharing keys between parties**, whereas public key encryption enables secure communication without the need for prior key exchange but is slower and computationally more intensive.



Private Key Encryption - Formal Definition

- A private-key encryption scheme is defined by a **message space M** and algorithms **(Gen, Enc, Dec)**
- **Gen (key-generation algorithm):** Generates key k
- **Enc (encryption algorithm):** takes key k and message me M as input; outputs cipher text c : **c← Enck(m)**
- **Dec (decryption algorithm):** takes key k and ciphertext c as input; outputs m : **m := Deck(c)**

Shift Cipher

(or Caesar Cipher)

Private Key Encryption

- Consider encrypting English text.
- Associate a with 0, b with 1, ..., z with 25.
- $k \in \{0, ..., 25\}$ This refers to the key, which can be any number between 0 and 25.
- To encrypt using key k, shift every letter of the plaintext by k positions (with wraparound). For instance, supposing the key is 3, ‘a’ would become ‘d’ (a shift of 3 places), ‘b’ would become ‘e’, and so on. ‘x’ would become ‘a’ and ‘y’ would become ‘b’ due to wraparound.
- Decryption is simply the reverse process.

Examples

- **Shift of 3 (k = 3):**
  - Plaintext: HELLO
  - Encrypted: KHOOR

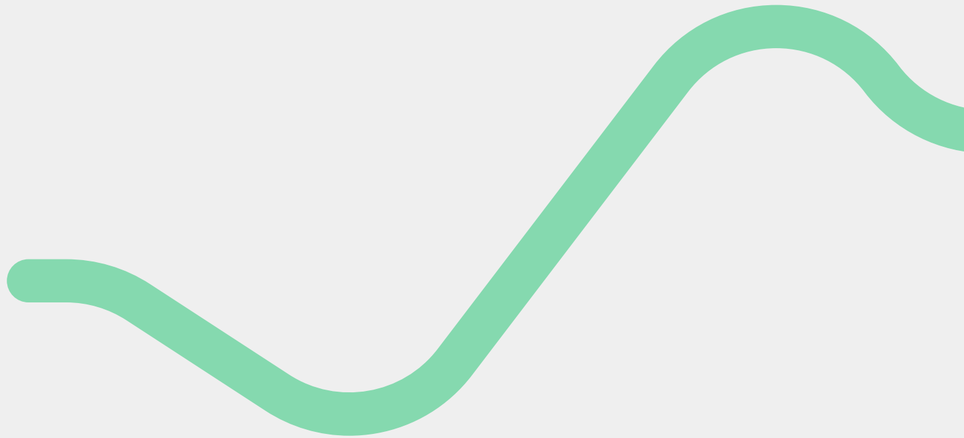
- **k = 5**:
  - Plaintext: OPEN SESAME
  - Encrypted: TUSJ XJXFRJ

- **k = 7**:
  - Plaintext: ENCRYPT THIS MESSAGE
  - Encrypted: LUKHTAV AOPZ TLZZHNL

- **k = 20**:
  - Plaintext: ALICE AND BOB
  - Encrypted: UZYSY SHN VYR

Now, if you are given an encrypted message and you know it is encrypted using shift cipher,

- What will be k, ie. the shift?
- How will you find the original message or the decrypted message?
- What will be the time complexity to find the original message?



Now, if you are given an encrypted message and you know it is encrypted using shift cipher,

- **What will be k, ie. the shift?**
- **How will you find the original message or the decrypted message?**
- **What will be the time complexity to find the original message?**

1. ‘K’ could be randomly selected from (0,25) and so there are 26 possible values of K.

Now, if you are given an encrypted message and you know it is encrypted using shift cipher,

- **What will be k, ie. the shift?**
- **How will you find the original message or the decrypted message?**
- **What will be the time complexity to find the original message?**

- ‘K’ could be randomly selected from (0,25) and so there are 26 possible values of K.
- We can loop over all 26 values of K, shift the encrypted message by -K places and find possible original message. Only the one intelligible would be the actual message.

Now, if you are given an encrypted message and you know it is encrypted using shift cipher,

- **What will be the time complexity to find the original message?**

- The time complexity to decrypt a shift cipher is O(n), where n is the length of the cipher text.
- This is because decrypting a shift cipher involves simply shifting each letter of the ciphertext back by the same fixed amount used in encryption. Since each character in the ciphertext is processed individually, the time complexity grows linearly with the length of the ciphertext.

In Big O notation, O(f(n)) represents the upper bound of the growth rate of a function f(n), where n is the size of the input. It describes the worst-case scenario for the algorithm's performance in terms of time or space.

Our Goal with Cryptography?

"Regardless of any prior info. the attacker has about the plaintext, the ciphertext should leak no additional information about the plaintext"

More formally...

Perfect secrecy

Encryption scheme (Gen, Enc, Dec) with message space M and ciphertext space C is perfectly secret

IF

for every distribution over M, every $m \in M$, and every $c \in C$ with $Pr[C=c] > 0$, it holds that

$$Pr[M = m \mid C = c] = Pr[M = m]$$

Some Probability...

- **Random variable** – variable that takes on (discrete) values with certain probabilities
- **Probability distribution for a r.v.** - specifies the probabilities with which the variable takes on each possible value
- **Each probability must be between 0 and 1**
- **The probabilities must sum to 1**

Some Probability...

- **Event** - a particular occurrence in some experiment
- **Pr[E]** - probability of event E
- **Conditional probability** - probability that one event occurs, assuming some other event occurred
- **Pr[A | B] = Pr[A and B] / Pr[B]**
- Two r.v.'s X, Y are independent if for all x, y:

$$\mathbf{Pr[X=x \mid Y=y] = Pr[X=x]}$$

Some Probability...

Law of total probability

- It states that if a sample space S can be partitioned into events E_1, E_2,..., E_n, then the probability of any event A can be calculated by

$$\Pr(A) = \Sigma_1 \Pr(A|E_1) * \Pr(E_1)$$

An Example

- **Consider the shift cipher**
- So for all k ∈ {0, …, 25}, **Pr[K = k] = 1/26**
- Say **Pr[M = 'a'] = 0.7**, **Pr[M = 'z'] = 0.3**

What is Pr[C = 'b'] ?

- **Pr[C='b'] = Pr[M='a']·Pr[K=1] + Pr[M='z'] ·Pr[K=2]**
  = 0.7 (1/26) + 0.3 (1/26) = 1/26

Does Shift Cipher meet definition of prefect secrecy?

- Consider the shift cipher, and the distribution Pr[M = 'one'] = ½, Pr[M = 'ten'] = 1/2
- Take m = 'ten' and c = 'rqh'

Pr[M = 'ten' | C = 'rqh'] = ?

= 0

≠ Pr[M = 'ten']"

> Therefore, shift cipher does not follow the definition of perfect secrecy!

I’ve Got Nothing to Hide

[Link to the paper]

"I've Got Nothing to Hide" and Other Misunderstandings of Privacy, written by Daniel J. Solove, challenges common misconceptions about privacy. He argues that privacy is not solely about hiding wrongdoing but encompasses broader values such as autonomy, trust, and individuality. The paper refutes arguments that dismiss privacy concerns, emphasizing its importance for fostering creativity, free expression, and democratic values. Solove advocates for a nuanced understanding of privacy in society, calling for legal and social frameworks that prioritize its protection while balancing competing interests.

!! Do give it a read !!

THANK YOU :)