VOL- VII ISSUE- XI NOVEMBER 2020 PEER REVIEW e-JOURNAL IMPACT FACTOR 6.293 ISSN 2349-638x

An Introduction to Mathematical Cryptography

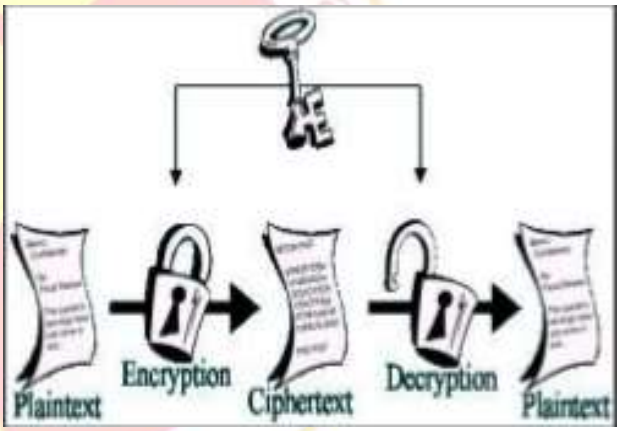
Dr. Siddharth Sudhakarrao Howal,
Assistant professor,
Dr.S.S.M.Pratishthan's
College Of Education, Ahmedpur Dist. Latur

Abstract:

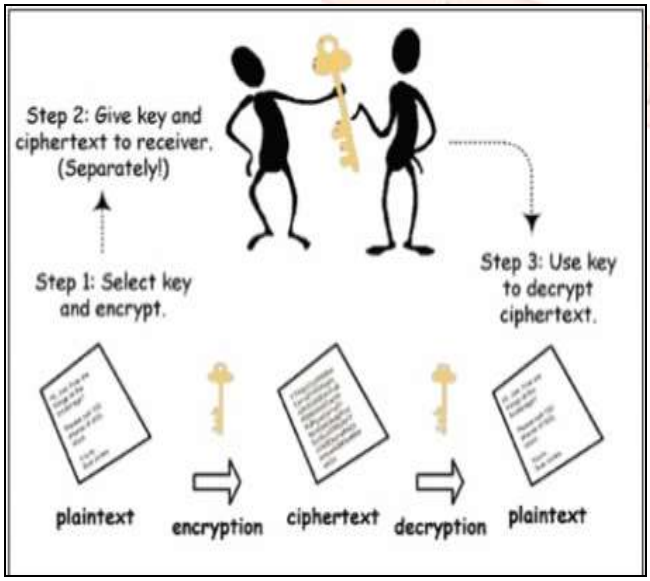
This paper provides a self-contained introduction to mathematical foundation of cryptography, with an emphasis on the mathematics behind the theory of public key. The paper focuses on *Steps involved , working* of cryptography. The science of using mathematics to encrypt and decrypt data, includes some techniques in the form of microdots, merging words sometimes with image, and other ways to hide information in storage.

Introduction:-

Cryptography is the science of using mathematics to encrypt and decrypt data. In other words, it is a old art or technique to write secret message. Cryptography comes from Greek word "crypto" means hiding and "Graphy" means writing. cryptography is method in which storing and transmitting data at a particular form so that only predefined can understood and process it. Cryptography includes some techniques in the form of microdots, merging words sometimes with image, and other ways to hide information in storage.



Steps involved in Cryptography:



Encryption : Encryption is nothing but, the coding information which may be a file or mail message in the cipher text , which is in a form not readable by anyone.

Decryption: decryption is a reverse process of encryption such as converting encoded data to its original form.

Plaintext : plaintext is the original message, before is being transformed.

After the message is transformed it is called as ciphertext.

An encryption algorithm transforms plaintext into ciphertext and decryption algorithm transforms that ciphertext back into plaintext. Encryption and decryption algorithms are referred as Ciphers. Also used to refer to different categories of algorithms in cryptography.

We take a glance, assigning Numerical Values to every alphabets i.e lower to upper a to z. The lower case is user for plaintext and upper case is used for ciphertext.

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

Key : A key is a number or a set of numbers that the cipher operates on it, just like algorithm.

To encrypt a message , we need an encryption algorithm, an encryption key and the plaintext.

Also to decrypt a message, we need to be a decryption algorithm, a decryption key and the plaintext.

Working Of Cryptography :

For Example :

we are using additive cipher with key = +15 to encrypt message “hello”.

We apply the encryption algorithm to plaintext, character by character as shown.

Plaintext: h ---> 07	Encryption (07+15=22)mod 26	Ciphertext: 22--- > W
Plaintext: e ---> 04	Encryption (04+15=19)mod 26	Ciphertext: 19--- > T
Plaintext: l ---> 11	Encryption (11+15=26)mod 26	Ciphertext: 00--- > A
Plaintext: l ---> 11	Encryption (11+15=26)mod 26	Ciphertext: 00--- > A
Plaintext: o ---> 14	Encryption(14+15=29)mod 26	Ciphertext: 03--- > D

Therefore, the plaintext “hello” is encrypted to ciphertext **“WTAAD”.**

PURPOSE OF CRYPTOGRAPHY :

1. **AUTHENTICATIN**
2. **PRIVACY / CONFIDENTIALITY**
3. **INTEGRITY**
4. **NON-REPUDIATION**

APPLICATION OF CRYPTOGRAPHY :

1. **SECURE COMMUNICATION :**
   To prevent eavesdropping war time communication and business transactions.
2. **IDENTIFICATION & AUTHENTICATION :**
   Checking the integrity.
3. **SECRET SHARING / DATA HIDING:**
   Hide something that has been written.
4. **KEY RECOVERY :**
   This technology allows a key to be revealed under certain circumstances without the owner of the key revealing it.
5. **REMOTE ACCESS :**
   Passwords gives a lever of security for secure access.

6. **CELL PHONES :**
   Prevent people from stealing cell phone numbers, access code .
7. **ACCESS CONTROL :**
   Regulate access to satellite and cable TV.

References:

1. Alfred J. Menezes, Jonathan Katz, Paul C. van Oorschot, Scott A. Vanstone (1996), Handbook of Applied Cryptography, CRC Press.
2. Hoffstein, Jeffrey, Pipher, Jill, Silverman, J.H. (2008),An Introduction to Mathematical Cryptography,LLC
3. Jean-Philippe, Aumasson (2017), Serious Cryptography, Kindle Edition