CRYPTOGRAPHY:A NEW VIEW POINT

PRATYUSHA VEDALA, SRI HARSHA RACHETI

[1,2]STUDENT (III B.TECH), COMPUTER SCIENCE & ENGINEERING, ANDHRA LOYOLA INSTITUTE OF ENGINEERING AND TECHNOLOGY ,VIJAYAWADA(A.P), INDIA

Email:pratyushavedala@gmail.com, rachetisriharsha@gmail.com

ABSTRACT-

Many Organizations are doing their best in keeping away from the threats of message hacking through various trends in Cryptography. However, of late, we are witnessing the message passing disasters more often than before .Here we would like to review this problem and discuss certain possible solutions. While hackers are using malicious techniques, the Cryptographic Industry is quickly responding to these threats in keeping away from these techniques. These Organizations are establishing strict cryptographic technics and placing them on the desk top. However, it is like closing all the doors of a House while keeping windows and other entry points open for these hackers. Now, we discuss about three basic Algorithms viz Private Key Algorithm, Public Key Algorithm and hash functions. Many discussions took place on the draw backs of Classical Cryptography and finally ensuring the need for going to new trends such as Quantum Cryptography and Elliptic Curve Cryptography. With these new technics, there is a hope that we can overcome the problems that we are facing in a head hoc way .By adopting these proven Technologies, with focus on manageability, we can meet the demanding situations by developing easy to use interfaces over a period of time through customer feedback.With the above advancement in the cryptography technics, we can be rest assured that , the secrecy involved in message passing can be saved from the clutches of the message hackers.

KEYWORDS-- cipher, plain text, encryption, decryption, private ke, public key.

INTRODUCTION

The global internet is the worldwide hub of network of computers. IANA superintends the addresses of the network of computers. It is witnessed a histrionic growth as it permits the possibility of entrance of anyone into the hub and also such connected people can get others connected to the network. Many dimensions can be defined to security and many applications for password protection, ecommerce and payments. One of the primary dimensions for the establishment of a secured communication is cryptography .The two prime motives of this paper being definition of basic concepts behind cryptographic methods is vague today and permission of multitude of Examples which pertain to real and emerging trends. A site connected to this hub can act as an ISP to the other site .Increased security may comfort overly suspicious people .On the other hand others feel the protections provides are very basic that are too naïve to believe .Presently the internet is facilitating transactions and is being used as a platform for commerce, security becomes a critically important issue.

WHAT IS CRYPTOGRAPHY?

Cryptography Provides Confidentiality, Integrity and Accuracy.
The word Kryptos is the root word for Cryptography meaning "Hidden Secrets".
It's all about hiding information.
Cryptography is the art of converting comprehensible data into an unintelligible one and again retransfiguring it into it's original form.

PURPOSE OF CRYPTOGRAPHY

On the development of computer communications the new forms cryptography has arised. Cryptography is very essential for data and telecommunications when communicating over a network especially the "Internet".
The pre-requisites of any application-application communication include:
Authentication: It is defined as veracity.
Privacy/Confidentiality: To make sure that only the authorized receiver can read.
Integrity: making sure that message received is unaltered or original.

Non –repudiation**:** A process that tells that message has been sent by the receiver

CONFIDENTIALITY
SECURITY
INTEGRITY
NON-REPUDIATION

Fig.1 SECURITY GOALS

Besides protecting the data from being theft or altered it also is used in user authentication.
The schemes that are generally used to achieve the above goals are as follows:
Secret key (symmetric) cryptography
Public key (assymetric) cryptography
Hash functions
They include plain text which is being encrypted into cipher text which will be decrypted into plain text for usage.
The crypto field consists of common, easier literature to identify the communicating parties called Alice and Bob

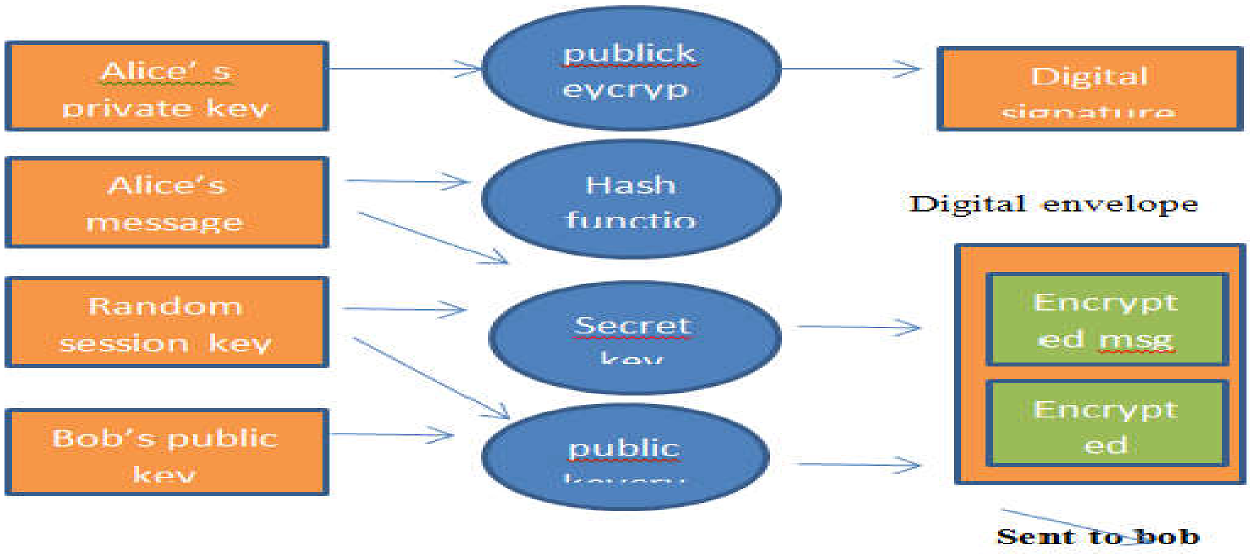


FIG.2 CRYPTOGRAPHY ARCHITECTURE

CRYPTOGRAPHY NOMENCLATURE

SECRET KEY CRYPTOGRAPHY
This is the symmetric encryption wherein a single key used for encryption and decryption functions.
Here the key would be known by both the receiver as well as sender
It might get harder for sharing a secret key
PUBLIC KEY CRYPTOGRAPHY
Public key is any of the keys given to each person
It can be easily looked up as it is published in an open directory

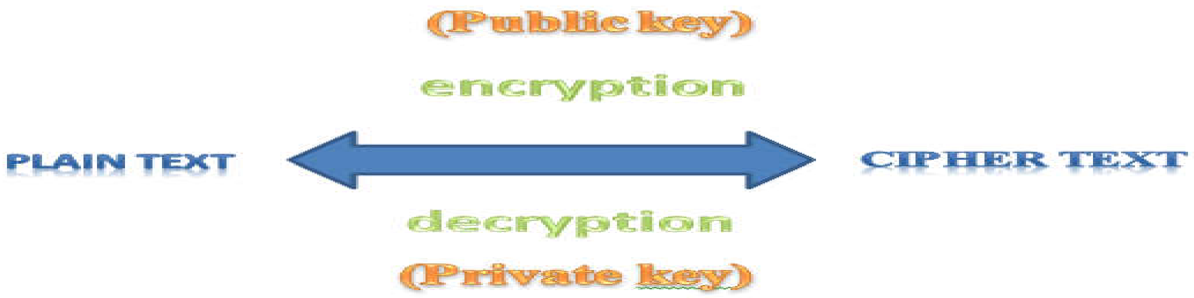
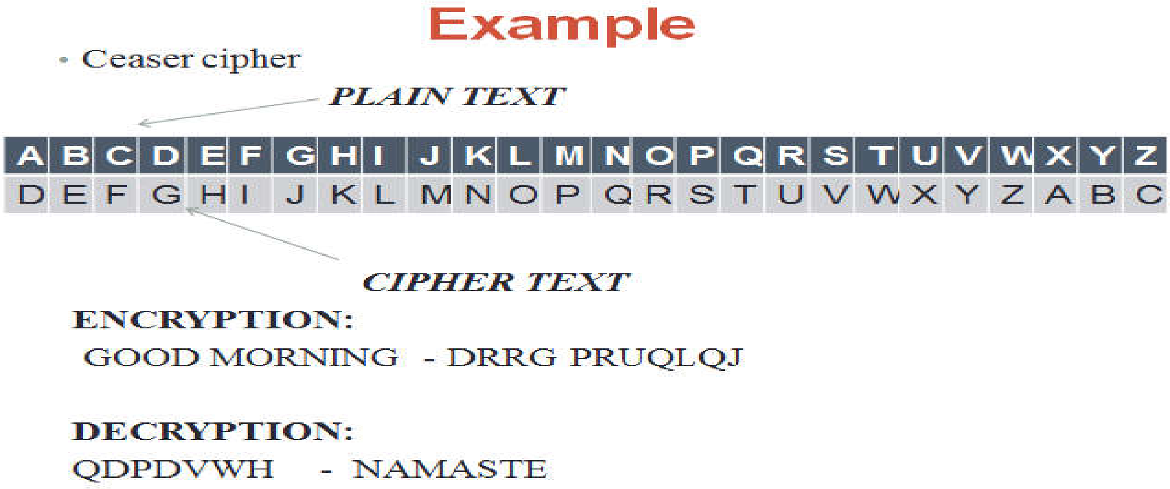


Fig.3 using of key

It involves:

- Encryption: conversion of plain text to cipher text
- *Decryption*: conversion of cipher text to plain text
- *Plain text* :text entered at the source
- *Cipher text* : encrypted plain text
- There are various ciphers
-



Example

- Ceaser cipher

PLAIN TEXT

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

CIPHER TEXT

ENCRYPTION:

GOOD MORNING - DRRG PRUQLQJ

DECRYPTION:

QDPDVWH - NAMASTE

ALGORITHMS

PUBLIC/PRIVATE KEY CRYPTOGRAPHY

The problem of key management is subdued by the use of encryption and decryption key pairs the knowledge of both these key pairs is a must.

As the name itself says public/private key cryptography the encryption key can be made public subject to the fact that decryption key is to be kept only by the party wishing to receive the encrypted message.

Named after Ronald , Shamir and Adleman RSA is a popularly used public/private key algorithm.

It is based on the factoring of the product of two very large prime numbers.

In El Gamal another public/private key algorithm we use discrete logarithm problem which is a different arithmetic algorithm.

A message which is encrypted with a public key can be decrypted only with the help of private key.

The converse also holds good.

RSA

- Named after Ronald ,Shamir and Adleman RSA is a popularly used public/private key algorithm based on the factoring of the product of two very large prime numbers
  c=p ^e mod n
  p=c ^d mod n
  n= p * q where, p & q are any two distinct prime numbers
  e – Public key

HASH FUNCTION

- It is a function that gets easier in calculating but gets harder in inverting it. Hence ,it is a one-way function
- Here the ability of the function to withstand attacks is being evaluated and the functions are then categorized on that basis.
- The hash functions with respect to the messages x and y are H(x) and H(y) respectively.
- There are 2 types of hash functions namely
- A strongly collision free hash function
- A weakly collision free hash function
- It produces a fixed length string as output in spite of taking a long string or a message of varied length that can be termed as a message digest or a digital finger print.
-

DATA ENCRYPTION STANDARD (DES):

- It is published in 1977 and standardized in 1979.
- Key: 64 bit->56+parity bits.
- It takes 64 bits as input and gives 64 bits as output.

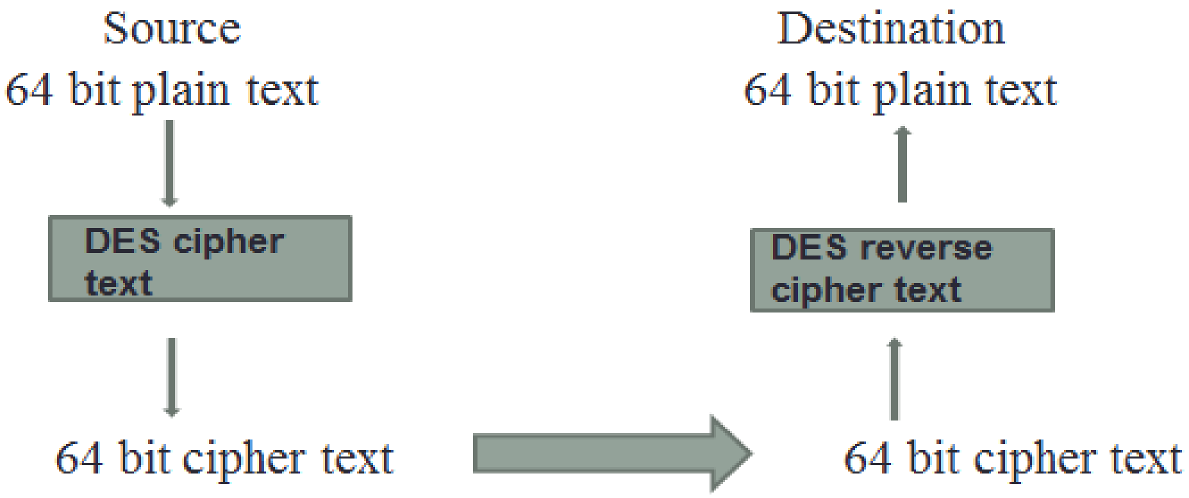
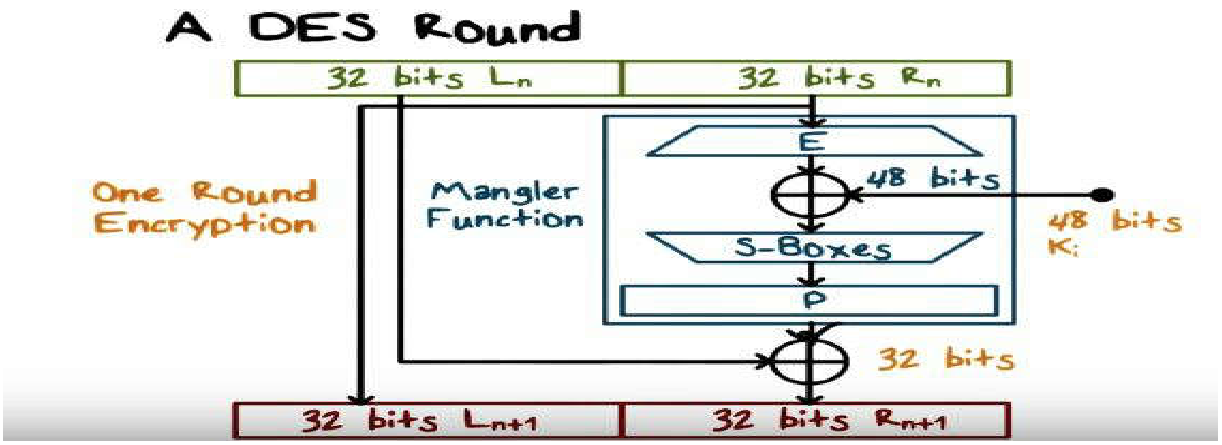


FIG.5 data encryption standard DES operation



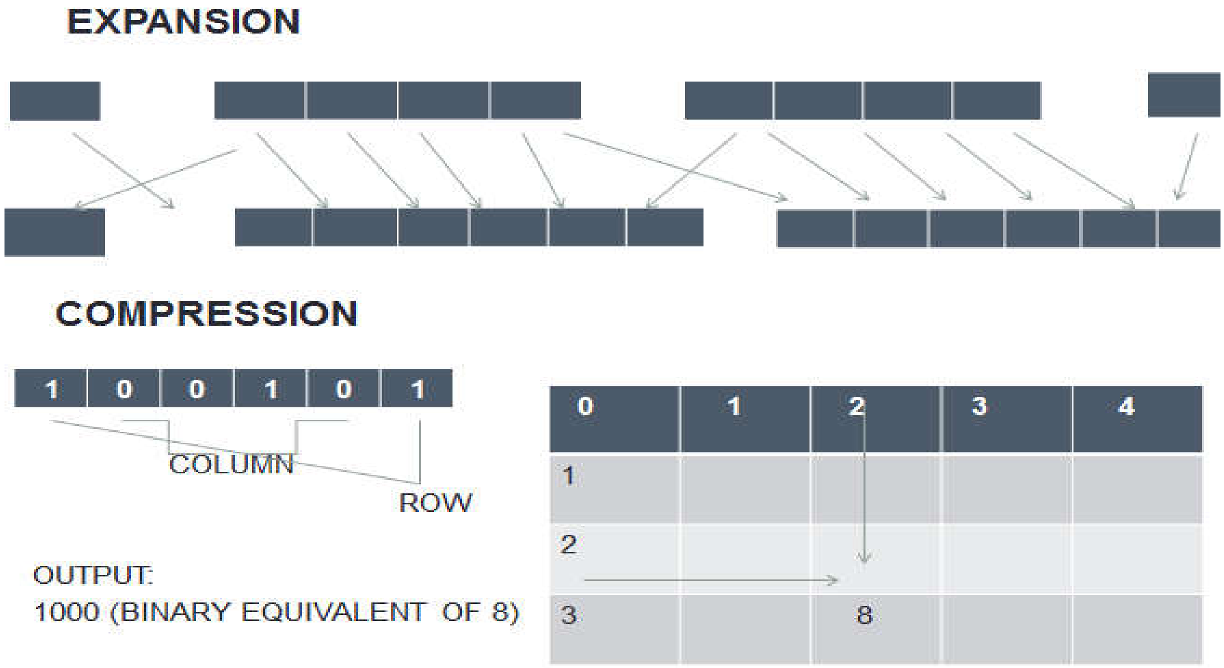
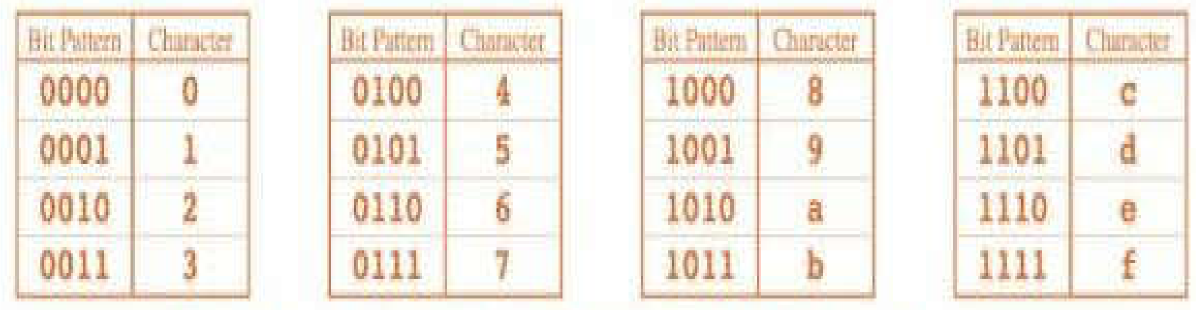


FIG.7 example of expansion and compression

ADVANCED ENCRYPTION STANDARD

- Also known by its original name Rijndael used for specification electronic data
- KEY SIZE-128
- BLOCK SIZE-128 ,192 , 256 & ROUNDS – 10 , 12 ,14
- Internally AES’ operations are performed on a 2D array of bytes called State.
- The basic unit in the processing in aes is a byte



Bit Pattern	Character	Bit Pattern	Character	Bit Pattern	Character	Bit Pattern	Character
0000	0	0100	4	1000	8	1100	c
0001	1	0101	5	1001	9	1101	d
0010	2	0110	6	1010	a	1110	e
0011	3	0111	7	1011	b	1111	f

Figure 1. Hexadecimal representation of bit patterns.

In the *SubBytes* step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S; bij = S(aij).

In the *ShiftRows* step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.

In the *MixColumns* step, each column of the state is multiplied with a fixed polynomial {\displaystyle c(x)} c(x).

In the *AddRoundKey* step, each byte of the state is combined with a byte of the round subkey using the XOR operation (⊕).

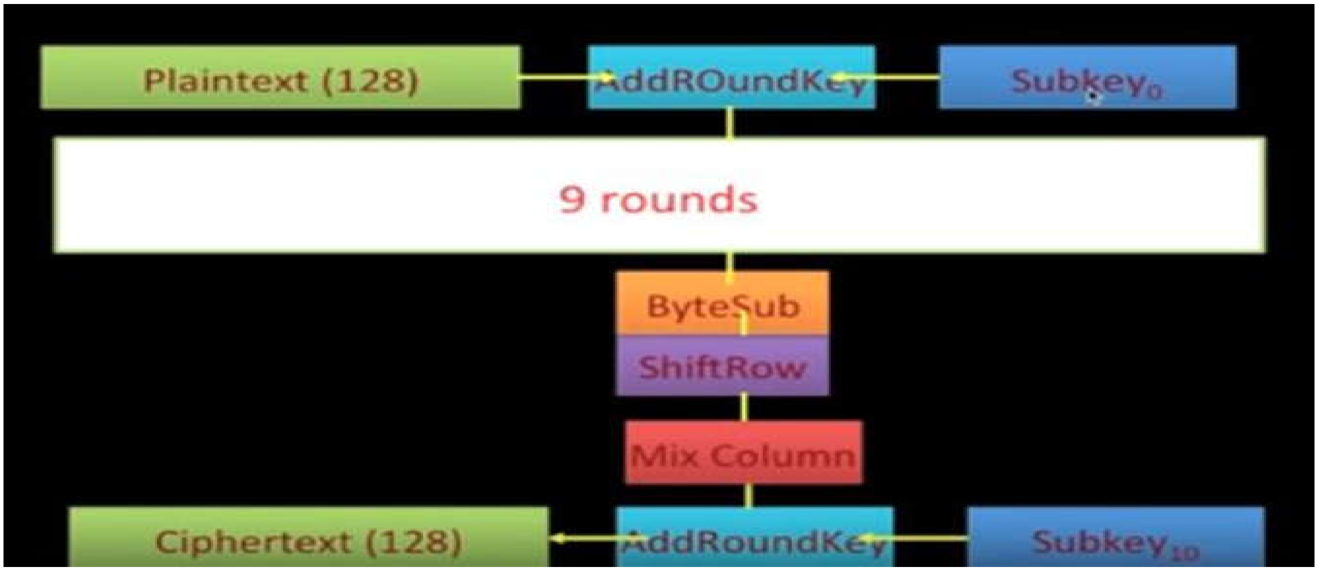


FIG.8 flow chart of AES

APPLICATIONS

- Defense services
- Secure data manipulation
- E –commerce
- Business transactions
- Internet payment systems
- User identification systems
- Access control
- Data security

CONCLUSION

In order to send confidential messages we use the public key algorithm on the other hand to send messages in a quicker manner private key algorithm is being used As per the requirement, public key or private key cryptography are to be chosen. For the establishment of security services different types of algorithms are used.

ACKNOWLEDGEMENT

We would like to extend our sincere thanks of gratitude towards our parents and the professors of our college ,Andhra Loyola Institute of Engineering and Technology.

REFERENCES

http://studymafia.org/wp-content/uploads/2015/01/CSE-Cryptography-report.pdf
https://www.slideshare.net/kusum21sharma/cryptographyppt
www.google.com
www.wikepedia.com

BIOGRAPHY

PRATYUSHA VEDALA **(***FIRST AUTHOR)*

Completed schooling in Nirmala High School Vijayawada and Intermediate in Sri Chaitanya Educational Institutions Vijayawada Currently pursuing 3rd year B.tech in Andhra Loyola Institute of Engineering and Technology Vijayawada (affiliated to JNTUK) with distinction in 1st two years' aggregate .Participated in some of the inter college competitions and presented papers onInternet Of Things(IOT),Facebook , Cicret Bracelet , E-Commerce , Machine Learning.

SRI HARSHA RACHETI ***(****SECOND AUTHOR)*

Completed schooling in Care And Share A and intermediate in Chaitanya junior College Gannavaram Currently pursuing 3rd year B.tech in Andhra Loyola Institute of Engineering and Technology Vijayawada (affiliated to JNTUK) with first class in 1st two years' aggregate .Gave seminars on Big Data-Hadoop and Humanoids –Robotics