An Overview on Cryptography with Symmetric & Asymmetric Encryption

[1]Prof. Amruta Navale, [2]Prof. Bharati Bhamare, [3]Prof. Sneha Sawant
[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor
[1]Dr. D.Y.Patil SCS College, Akurdi, Pune-44,
[2]Dr. D.Y.Patil ACS College, Pimpri ,Pune-18,
[3]Dr. D.Y.Patil ACS College, Pimpri ,Pune-18

Abstract **- Cryptography is one such technique that permits secure information transmission while not losing its confidentiality and integrity. Supported the key distribution, cryptography is more classified into 2 major types- Symmetric Key Cryptography and uneven Key Cryptography. During this paper, we've surveyed the normal algorithms, beside the projected algorithms supported their professionals and cons, associated with regular and uneven Key Cryptography. We've conjointly compared the importance of each these scientific discipline techniques. The projected algorithms verified to be extremely economical in their various grounds however there ar sure areas that remained open associated with these algorithms, and haven't nonetheless been completely mentioned.**

keywords **- Crypto,Key,Plain text,Cipher text,encyption,Decryption,Security,Integrity, Symmetric, Asymmetric**

I.INTRODUCTION

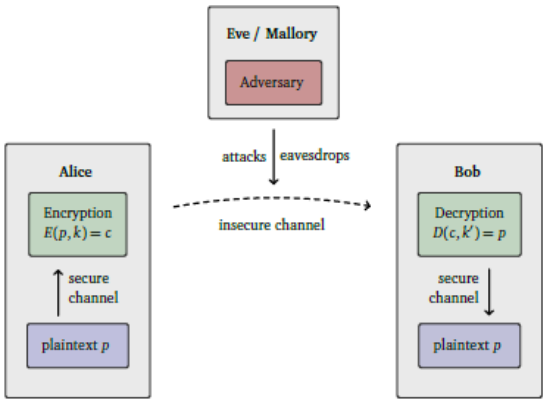
Cryptography may be a methodology of protective data and communications through the utilization of codes in order that solely those for whom the knowledge is meant will browse and method it. The pre-fix "crypt" means that "hidden" or "vault" and therefore the suffix "graphy" stands for "writing."

In computing, cryptography refers to secure data and communication techniques derived from mathematical ideas and a collection of rule-based calculations referred to as algorithms to rework messages in ways in which square measure laborious to decipher. These settled algorithms square measure used for cryptographical key generation and digital sign language and verification to safeguard knowledge privacy, internet browsing on the net and confidential communications like master card transactions.

II.CRYPTOGRAPHY FUNCTIONS

Cryptography is that the study of mathematical techniques associated with aspects of data security like confidentiality, knowledge integrity, entity authentication and knowledge origin authentication. Therefore the main goals of cryptography square measure privacy or confidentiality, knowledge integrity, authentication and non-repudiation.

- **Privacy/confidentiality:** Ensuring that nobody will browse the message except the meant receiver. data will solely be accessed by the person for whom it's meant and no different person except him will access it. Secrecy, confidentiality and privacy square measure substitutable terms. There square measure variety of eleven approaches to providing confidentiality through mathematical algorithms that renders knowledge unintelligible.
- **Authentication:** The method of proving one's identity. The identities of sender and receiver square measure confirmed. Yet as destination/origin of data is confirmed.
- **Integrity**: Assuring the receiver that the received message has not been altered in any approach from the initial. Data can't be changed in storage or transition between sender and meant receiver with none addition to data being detected.. **Data integrity** refers to the unauthorized manipulation of information. knowledge manipulation includes such things as insertion, deletion and substitution. It ensures the power of sleuthing knowledge manipulation by unauthorized parties.
- **Non-repudiation**: A mechanism to prove that the sender extremely sent this message. The creator/sender {of data|of data|of knowledge} cannot deny his or her intention to send information at later stage.
- **Key exchange**: The methodology by that crypto keys square measure shared between sender and receiver.
  In cryptography, we tend to begin with the unencrypted knowledge, stated as plaintext.
- **Plaintext** is encrypted into cipher text, which can successively (usually) be decrypted back into usable plaintext. The coding and coding relies upon the kind of cryptography theme being utilized and a few sort of key.
- This is supported strategies like coding, decryption, signing, generating of pseudo random numbers, etc.



.

III. PARTS OF A CRYPTOGRAPHY

A. **Plaintext.** it's the info to be protected throughout transmission.

B. **(Encryption) Coding formula**. it's a mathematical operation that produces a ciphertext for any given plaintext and coding key. it's a cryptographical formula that takes plaintext Associate in Nursingd an coding key as input and produces a ciphertext.

C. **Ciphertext.** It's the disorganised version of the plaintext made by the coding formula employing a specific the coding key. The ciphertext isn't guarded. It flows on public channel. It is intercepted or compromised by anyone UN agency has access to the communicating.

D. **(Decryption)Coding formula**, it's a mathematical operation, that produces a singular plaintext for any given ciphertext and coding key. it's a cryptographical formula that takes a ciphertext and a coding key as input, and outputs a plaintext. The coding formula basically reverses the coding formula and is therefore closely associated with it.

E. **Encryption Coding Key.** it's a worth that's proverbial to the sender. The sender inputs the coding key into the coding formula together with the plaintext so as to calculate the ciphertext.

F. **Decryption Coding Key**. it's a worth that's proverbial to the receiver. The coding secret's associated with the coding key, however isn't continually a dead ringer for it. The receiver inputs the coding key into the coding formula together with the cipher text so as to calculate the plaintext.

G. **Interceptor** (an attacker) is Associate in Nursing unauthorized entity UN agency makes an attempt to see the plaintext. He will see the ciphertext and should grasp the coding formula. He, however, must not ever grasp the coding key.

IV. SORTS OF CRYPTOSYSTEMS

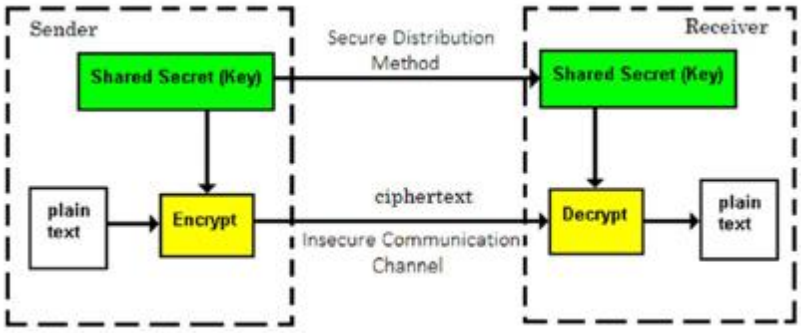
1. Symmetric Key Encryption
2. Asymmetric Key Encryption

Symmetric Key Encryption:

Symmetric Key Encryption The encryption process where same keys are used for encrypting and decrypting the knowledge is understood as Symmetric Key Encryption.

The salient features of cryptosystem supported symmetric key encryption are:

- Persons using symmetric key encryption must share a standard key before exchange of data .
- Keys are recommended to be changed regularly to stop any attack on the system
- a strong mechanism must exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.
- during a group of n people, to enable two-party communication between any two persons, the amount of keys required for group is n *(*n- 1)/2.
- Length of Key (number of bits) during this encryption is smaller and hence, process of encryption-decryption is quicker than asymmetric key encryption.
- Processing power of computing system required to run symmetric algorithm is a smaller amount .
- Key establishment -Before any communication, both the sender and therefore the receiver got to agree on a secret symmetric key. It requires a secure key establishment mechanism in situ .
- Trust Issue -Since the sender and therefore the receiver use an equivalent symmetric key, there's an implicit requirement that the sender and therefore the receiver.

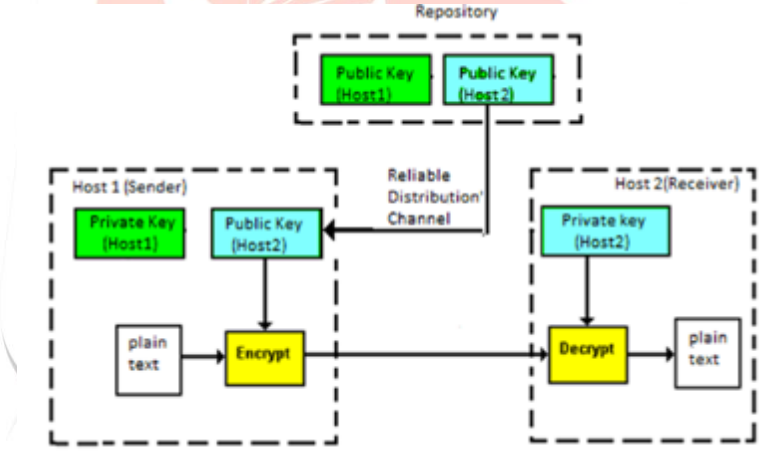


Asymmetric Key Encryption :

The encryption process where different keys are used for encrypting and decrypting the knowledge is understood as Asymmetric Key Encryption. Though the keys are different, they're mathematically related and hence, retrieving the plaintext by decrypting ciphertext is possible . Asymmetric Key Encryption was invented within the 20th century to return over the need of pre-shared secret key between communicating persons.

The salient features of this encryption scheme are as follows:

- It requires to place the general public key publicly repository and therefore the private key as a well-guarded secret. Hence, this scheme of encryption is additionally called Public Key Encryption.
- Though public and personal keys of the user are related, it's computationally not feasible to seek out one from another. this is often a strength of this scheme
- When Host1 must send data to Host2, he obtains the general public key of Host2 from repository, encrypts the info , and transmits.
- Host2 uses his private key to extract the plaintext.
- Length of Keys (number of bits) during this encryption is large and hence, the method of encryption-decryption is slower than symmetric key encryption.
- Processing power of computing system required to run asymmetric algorithm is higher. The technology comes in many forms, with key size and strength generally being the most important differences in one variety from subsequent.



V.ALGORITHMS OF ENCRYPTION

1) Triple DES

Triple DES was designed to exchange the first encoding Standard (DES) algorithm, which hackers eventually learned to defeat with relative ease. At just one occasion, Triple DES was the recommended standard and therefore the most generally used symmetric algorithm within the industry.

Triple DES uses three individual keys with 56 bits each. The entire key length adds up to 168 bits, but experts would argue that 112-bits in key strength are more love it.

Despite slowly being phased out, Triple DES still manages to form a dependable hardware encryption solution for financial services and other industries.

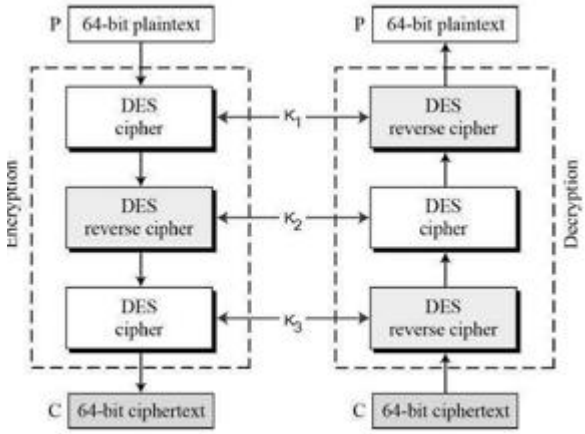
The pragmatic approach wasn't to abandon the DES completely, but to vary the way during which DES is employed . This led to the modified schemes of Triple DES (sometimes referred to as 3DES).

Incidentally, there are two variants of Triple DES referred to as 3-key Triple DES (3TDES) and 2-key Triple DES (2TDES).

3-KEY Triple DES

Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys K1, K2 and K3. this suggests that the particular 3TDES key has length 3*56 = 168 bits.

The encryption scheme is illustrated as follows :



Block cipher with symmetric secret key

Block length = 64 bits

Key length = 56, 112, or 168 bits.

The encryption-decryption process is as follows :

*Encrypt the plaintext blocks using single DES with key K1.

* Now decrypt the output of step 1 using single DES with key K2.

* Finally, encrypt the output of step 2 using single DES with key K3.

The output of step 3 is that the ciphertext.

* Decryption of a ciphertext may be a reverse process. User first decrypt using K3, then encrypt with K2, and eventually decrypt with K1.

Due to this design of Triple DES as an encrypt-decrypt.encrypt process, it's possible to use a 3TDES (hardware) implementation for single DES by setting K1, K2, and K3 to be an equivalent value. This provides backwards compatibility with DES.

Second variant of Triple DES (2TDES) is just like 3TDES except that K3is replaced by K1. In other words, user encrypt plaintext blocks with key K1, then decrypt with key K2, and eventually encrypt with K1 again. Therefore, 2TDES features a key length of 112 bits.

There are three keying options in encoding standards:

1. All keys being independent
2. Key 1 and key 2 being independent keys
3. All three keys being identical

Triple DES systems are significantly safer than single DES, but these are clearly a way slower process than encryption using single DES.

2) RSA

RSA may be a public-key encoding formula and also the commonplace for encrypting knowledge sent over the web. It conjointly happens to be one among the ways employed in our PGP and GPG programs.

Unlike Triple DES, RSA is taken into account Associate in nursing uneven formula thanks to its use of a combine of keys. You've got your public key, that is what we have a tendency to use to inscribe our message, and a personal key to decipher it. The results of RSA encoding may be a large batch of mumbo elephantine that takes attackers quite an little bit of time and process power to interrupt.

RSA is Associate in Nursing encoding formula, accustomed firmly transmit messages over the web. it's supported the principle that it's simple to multiply massive numbers, however resolution massive numbers is extremely troublesome. for instance, it's simple to visualize that thirty one and thirty seven multiply to 1147, however making an attempt to seek out the factors of 1147 may be a for much longer method.

RSA is Associate in Nursing example of public-key cryptography, that is illustrated by the subsequent example:

Suppose Alice needs to send Bob a valuable diamond, however the jewel are purloined if sent unsecured. each Alice and Bob have a range of padlocks, however they do not own a similar ones, which means that their keys cannot open the other's locks.

The implementation of RSA makes significant use of standard arithmetic, Euler's theorem, and Euler's to tient perform. Notice that every step of the formula solely involves multiplication, thus it's simple for a laptop to perform:

1. First, the receiver chooses 2 massive prime numbers pp and qq. Their product, n=pqn=pq, are 1/2 the general public key.
2. The receiver calculates phi(pq)=(p-1)(q-1)ϕ(pq)=(p−1)(q−1) and chooses variety electrical engineering comparatively prime to phi(pq)ϕ(pq). In apply, electrical engineering is usually chosen to be 2^+1=65537216+1=65537, although it will be as tiny as thirty three in some cases. electrical engineering are the opposite 1/2 the general public key.
3. The receiver calculates the standard inverse doctorate of electrical engineering modulo phi(n)ϕ(n).

In different words, First State equiv one pmod}de≡1(modϕ(n)). doctorate is that the personal key.
4. The receiver distributes each components of the general public key: nn and electrical engineering. doctorate is unbroken secret.
Now that the general public and personal keys are generated, they will be reused as typically as wished.

To transmit a message, follow these steps:

1. First, the sender converts his message into variety millimetre. One common conversion method uses the American Standard Code for Information Interchange alphabet:

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

2. For example, the message **"HELLO"** would be encoded as **7269767679**. it's vital that m<nmare lost once taken modulo nn, thus if nn is smaller than the message, it'll be sent in items.

3. The sender then calculates c equiv m^e pmodc≡me(modn). cc is that the ciphertext, or the encrypted message. Besides the general public key, this is often the sole data Associate in Nursing assailant are able to steal.

4. The receiver computes c^d equiv m pmod ncd≡m(modn), therefore retrieving the initial variety millimetre.

5. The receiver interprets millimetre back to letters, retrieving the initial message.

Key generation

The keys for the RSA formula area unit generated within the following way:
1. select 2 distinct prime numbers p and letter.
o For security functions, the integers p and letter ought to be chosen arbitrarily, and may be similar in magnitude however take issue long by a number of digits to form resolution tougher.[2] Prime integers will be expeditiously found employing a property check.
o p and letter area unit unbroken secret.

2. reckon n = pq.
o n is employed because the modulus for each the general public and personal keys. Its length, sometimes expressed in bits, is that the key length.
o n is discharged as a part of the general public key.

3. reckon λ(n), wherever wherever is Carmichael's totient perform. Since n = pq, λ(n) = lcm(λ(p),λ(q)), and since p and letter area unit prime, λ(p) = φ(p) = p − one and likewise λ(q) = letter − one. thence λ(n) = lcm(p − one, q − 1).
o λ(n) is unbroken secret.
4. select Associate in Nursing number e specified one < e < λ(n) and gcd(e, λ(n)) = 1; that's, e and λ(n) area unit coprime.
o e having a brief bit-length and tiny overacting weight ends up in additional economical encoding – the foremost usually chosen worth for e is 216 + one = sixty five,537. the littlest (and fastest) attainable worth for e is three, however such alittle worth for e has been shown to be less secure in some settings.[14]
o e is discharged as a part of the general public key.

5. confirm d as d ≡ e−1 (mod λ(n)); that's, d is that the standard opposite of e modulo λ(n).
o This means: solve for d the equation d · e ≡ one (mod λ(n)). d will be computed expeditiously by victimisation the Extended geometrician formula.
o d is unbroken secret because the personal key exponent.
The public key consists of the modulus n and also the public (or encryption) exponent e. The personal key consists of the personal (or decryption) exponent d, that should be unbroken secret. p, q, and λ(n) should even be unbroken secret as a result of they will be accustomed calculate d. In fact, they will all be discarded when d has been computed.

3) AES

The Advanced coding commonplace (AES) is that the formula sure because the commonplace by the U.S. Government and various organizations.
Although it's extraordinarily economical in 128-bit kind, AES additionally uses keys of 192 and 256 bits for significant duty coding functions.
AES is basically thought of fast to all or any attacks, with the exception of brute force, that tries to decipher messages victimization all potential mixtures within the 128, 192, or 256-bit cipher. Still, security consultants believe that AES can eventually be hailed the factual commonplace for encrypting information within the non-public sector.
A replacement for DES was required as its key size was too tiny. With increasing computing power, it had been thought of vulnerable against thorough key search attack. Triple DES was designed to beat this disadvantage however it had been found slow.

The options of AES square measure as follows −

• Symmetric key symmetrical block cipher
• 128-bit information, 128/192/256-bit keys
• Stronger and quicker than Triple-DES
• Provide full specification and style details
• Software implementable in C and Java

AES is associate unvarying instead of Feistel cipher. it's supported 'substitution–permutation network'. It includes of a series of connected operations, a number of that involve replacement inputs by specific outputs (substitutions) et al involve shuffling bits around (permutations).
• Interestingly, AES performs all its computations on bytes instead of bits. Hence, AES treats the 128 bits of a plaintext block as sixteen bytes.the longer term of coding Cyber attacks square measure perpetually evolving, therefore security specialists should keep busy within the research laboratory concocting new schemes to stay them unfree. skilled observers square measure hopeful that a replacement technique referred to as Honey coding can deter hackers by serving up faux information for each incorrect guess of the key code. This distinctive approach not solely slows attackers down, however doubtless buries the right key during a rick of false hopes. Then there square measure rising strategies like quantum key distribution, that shares keys embedded in photons over fiber optic, that may have viability currently and lots of years into the longer term yet.

VI.CONCLUSION

Cryptography is employed to attain few goals like Confidentiality, knowledge integrity, Authentication etc. of the send knowledge currently, so as to attain these goals varied science algorithms square measure developed by varied individuals. For a awfully nominal quantity of information those algorithms wouldn't be price effective since those don't seem to be designed for little quantity of information. The aim of this work was to style and implement a replacement algorithmic program to deal with this issue in order that we have a tendency to don't got to apply those algorithms (which don't seem to be cost-effective) to write in code a tiny low quantity of information. Keeping this goal in mind the projected algorithmic program has been designed during a quite easy manner however of-course not sacrificing the protection problems. one is employed for each secret writing and secret writing i.e. it's fallen underneath secret key science algorithmic program. However as public key cryptography is additional secured then secret key cryptography our next task would be to develop and style a public key science algorithmic program during a easy manner because it is completed during this paper.

REFERENCES

[1]" Cryptography and Network Security" – by Atul Kahate – TMH.
[2] "Data Communications and Networking"- by Behourz A Forouzan
[3] "Cyber Security Operations Handbook" – by J.W. Rittiaghouse and William M.Hancok – Elseviers.
[4] "Computer Networks Fourth Edition" – Andrew Tanenbaum
[5] "An Introduction to Cryptography" -Mohamed Barakat, Christian Eder, Timo Hanke blog.storagecraft.com/5-common-encryption-algorithms/
[6] cryptography/triple_des.html. Computer Network Security, Kizza, Springer
[7] "Cryptography and Network Security" Prentice Hall /Pearson Education By William Stallings