International Journal of Computing Academic Research (IJCAR)
ISSN 2305-9184, Volume 5, Number 1 (February 2016), pp.11-26

http://www.meacse.org/ijcar

A Survey on Elementary, Symmetric and Asymmetric Key Cryptographic Techniques

V.Hemamalini, G. Zayaraz, V.Susmitha, M.Gayathri and M.Dhanam

Dept of Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India

Abstract

Security is the most challenging aspects in the internet and network applications. Internet and network applications are growing faster. So the importance and the value of the exchanged data over the internet or other media types are increasing. The better solution to offer the necessary protection against the data intruders is cryptography. Cryptography is one of the main categories of computer security that converts information from its normal form into an unreadable form by using Encryption and Decryption Techniques. The Cryptography ensures that the message should be sent without any alternations and only the authorized person can be able to open and read the message. A numbers of cryptographic techniques are developed for achieving secure communication. There are basically two techniques of cryptography-Symmetric and Asymmetric. Symmetric encryption is the oldest and best-known technique. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key. The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret. This paper presents a detailed study of the symmetric and asymmetric techniques over each other.

Keywords – Cryptographic techniques, Symmetric, Asymmetric, Cipher text, public key, private key.

Introduction

Many personal data are shared through communication mediums like e-mail or WWW browsers over an internet. These browsers are not safe for sending and receiving information. Hence many websites provide secure private connection with the users by including personal information such as contact details [1]. Online users may need private and safety connection so as to prevent others from reading their emails and other personal data. Cryptography is an ancient art and it is the science of writing in secret code. In data and telecommunications, cryptography is must for communicating over any unsecured medium particularly the internet within the context of any applications–to–application communication there are some security requirements which includes,

Authentication: The process of providing one's identity.

Privacy / Confidentiality: Ensuring that no one can read the message except the intended user.

Integrity: Giving assurance to the receiver that the received message has not been altered from original

Non-Repudiation:A mechanism to prove that the sender send this message really.

Cryptography, then not only protects data from theft or alteration, but it also can be used for user authentication.In general, three types of cryptographic schemes are typically used to accomplish these goals:secret key (or symmetric cryptography), public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text which will in turn be decrypted into usable plaintext. There are several ways of classifying cryptographic algorithm [2].

(i)Secret Key: Users involved in the communication network make use of single key for encrypting and decrypting the messages.
(ii)Public Key: Users involved in the communication network make use of different keys for encrypting and decrypting the messages at both sides.
(iii)Hash Function: Hash function is a one way trapdoor function which is to map the arbitrary values to an some length.

ELEMENTARY CRYPTOGRAPHY

Cryptography is the best tool for controlling many secret threats. It is rooted in higher mathematics: group and field theory, computational complexity and real analysis. To use cryptography it is not important to know the underlying mathematics. Cryptography introduces the basic principles of encryption with 2 encryption methods: substitution and transposition. Then we have to explore how the encryption can be expanded to create stronger protection. We analyse the techniques used to break the protective scheme and get back the original plain text [12].Three algorithms like DES, AES and RSA are used as building blocks with protocols and structures to perform other tasks such as signing documents, detecting changes and exchanging personal data.

Basic encryption techniques of cryptography

There of two basic techniques for encrypting a message of plain text to cipher text they are as follows

1. Substitution Technique
2. Transposition Technique

1. Substitution Technique

In substitution technique plain text is replaced with cipher text based on some system (pairs of letters, triples of letters, etc) [13].The receiver then decrypts it by inverse substitution. There are many kinds of cipher:

Caesar Cipher Caesar cipher is also known as shift cipher [4]. It is a type of substitution cipher where each letter in plain text is replaced by a letter some fixed number of positions down the alphabet.

Example:Caesar cipher using a left rotation of three places, equivalent to a right shift of 23 (the shift parameter used is the key)

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

MonoalphabeticCipher :A monoalphabetic cipher also known as simple substitution cipher where the substitution is fixed for each letter of the alphabet [4]. If "a" is encrypted to "r" then every time "a" occurs in plain text it will be encrypted to "r".

Example

Plaintext Alphabet	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 Alphabet	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	A

Homoalphabetic Cipher In the Homophonic Substitution cipher single plain texts can be replaced by many cipher text letters [2]. Hence it is more difficult to break than standard methods. The number of characters each letter is replaced by is part of the key. As we allow more and more possible alternatives for each letter, the resulting cipher can be very secure [7].

Example

Plaintext Alphabet	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 Alphabet	1	8	F	R	E	S	H	T	O	M	A	N	D	2	9	C	U	B	G	I	J	K	L	P	Q	V	W	X	Y	Z	0	3	4	5	6	7

To encipher the message DEFEND THE EAST WALL OF THE CASTLE, we find 'D' in the top row, then replace it with the letter below it, 'F'. The second letter, 'E' provides us with several choices; we could use any of 'Z', '7', '2' or '1'. We choose one of these at random, say '7'. After continuing with this, we get the ciphertext.

Vigenere Cipher: The Vigenere Cipher is an example of a polyalphabetic cipher also called as running key cipher because the key is another text.Start with a key string: ―monitors to go to the bathroom and a plaintext to encrypt: ―four score and seven years ago. Align the two texts, possibly removing spaces: plaintext: fours core and seven years ago key: monitors to go to the bathroom cipher text: rcizlqfkxotrlsolrzetyjoua Then use the letter pairs to look up an encryption in a table (called a Vigen`ere Tableau or tabula recta).

Example

Blaise de Vigenère developed a square to help encode messages. Reading along each row, you can see that it is a really a series of Caesar ciphers the first has a shift of 1, the second a shift of 2 and so theVigenère cipher uses this table in conjunction with a key to encipher a message. So, if we were to encode a message using the key COUNTON, we write it as many times as necessary above our message. To find the encryption, we take the letter from the intersection of the Key letter row, and the Plaintext letter column.

Key	C	O	U	N	T	O	N	C	O	U	N	T	O	N
Plaintext	V	I	G	E	N	E	R	E	C	I	P	H	E	R
Encryption	X	W	A	R	G	S	E	G	Q	C	C	A	S	E

To decipher the message,the recipient needs to write out the key above the ciphertext and reverse the process.

The maths behind the Vigenère cipher can be written as follows:

To encrypt a message: Ca = Ma + Kb (mod 26)
To decrypt a message: Ma = Ca – Kb (mod 26)
(Where C = Code, M = Message, K = Key, and where a = the ath character of the message bounded by the message, and b is the bth character of the Key bounded by the length of the key.)

2. Transposition technique

Transposition technique is achieved by performing some kind of permutation on the plaintext letters. It is very simple to realize various this kind of cipher [8]. We can do it by the example. If the plaintext is "meet me after the party".

We can rearrange it by this way:

m e m a t r h p r y e t e f e t e a t

So we get the plaintext and the ciphertext like this:
plaintext: meet me after the party
ciphertext: mematrhpryetefetea

Rail fence cipher: The Rail Fence cipher is a form of transposition cipher where the plaintext is written downwards on successive rails of an imaginary fence as per the name.

Example

D				N				E				T				L		
	E		E		D		H		E		S		W		L		X	
		F				T				A				A				X

One-Time Pad Cipher: The one-time pad is the secure cryptosystem where the message is represented as binary string [10] .The encryption is done by adding the key to the message modulo 2, bit by bit. This process is known as exclusive or (XOR) [4] represented by truth table where + means "true" and – means "false". The cipher is reciprocal in that the identical key stream is used to both encipher the plain text and decipher cipher text to yield original text.

Plaintext ⊕ Key = Ciphertext and
Ciphertext⊕ Key = Plaintext

Example

Or sender is captured and claims the key is...

	s	r	l	h	s	s	t	h	s	r
Ciphertext:	110	101	100	001	110	110	111	001	110	101
"Key":	111	101	000	011	101	110	001	011	101	101
"Plaintext":	001	000	100	010	011	000	110	010	011	000
	h	e	l	i	k	e	s	i	k	e

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Running Cipher: In classical cryptography, the running key cipher is of polyalphabetic substitution cipher in which a text, typically from a book, is used to provide a very long key stream [11]. Usually, thebook to be used would be agreed ahead of time, while the passage to use would be chosen randomly for each message and secretly indicated somewhere in the message.

Example**:**

The running key is then written under the plaintext:

Plaintext: F l E e a t o n C e

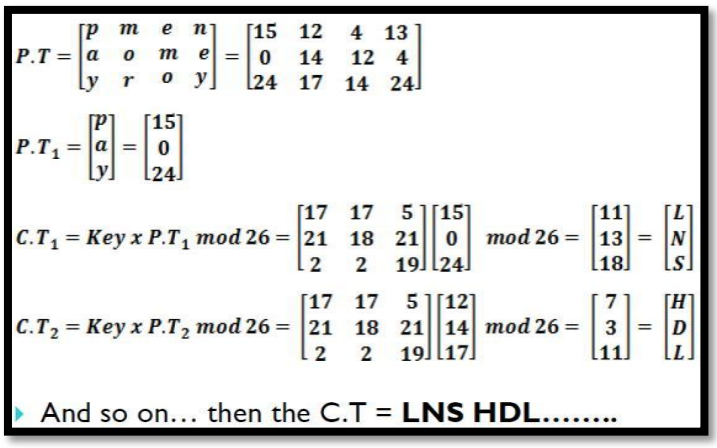
Running key: E R R O R S C A N O

Ciphertext: J C V S R L Q N P S

PlayFairCipherThistechnique encrypts pairs of letters instead of single letters. It is hard to break as the frequency analysis does not work with it. So it requires more cipher text to work [10].

Example**:**

Hill Cipher : Hill cipher uses linear algebra and requires little knowledge on matrices. Hence it has more mathematical nature than others. The concepts used are matrix Multiplication; Modular Inverses; Determinants of Matrices; Matrix Adjugates(for finding inverses)[10]. It can easily process larger blocks of letters.
Example



Block Cipher: The block cipher is based on iterated product cipher where it conducts operations over multiple rounds. In each round different sub key is used which is derived from original key. Secure block ciphers remain suitable for the encryption of one block of information using a fixed key.There have been numerous modes of operation developed for the cipher to allow repeated use in secure channels in order to achieve authenticity and confidentiality [18]. Block ciphers have also been used as the foundation protocol in more complex cryptographic protocols to include pseudo-random number generators and universal hashing functions. Feistal network implement this cipher.

Stream Cipher: Stream ciphers make use of a symmetric key that uses plaintext combined with a pseudorandom cipher digit stream also known as a key stream. It encrypts plain text one at a time along with corresponding key stream. The output will be the corresponding cipher text stream. It is also known as state cipher as every digit is dependent on current state of cipher [6]. A digit will be a bit and the combination operation will use the XOR operation. Pseudorandom key streams are normally created from a random seed value that uses digital shift registers. The seed value will also function as the key for decrypting the cipher stream. Unlike block ciphers, stream ciphers represent a different approach to encrypting and decrypting information. In order to avoid being cracked, stream ciphers should not use the same seed twice or else and adversary may be able to crack the code.

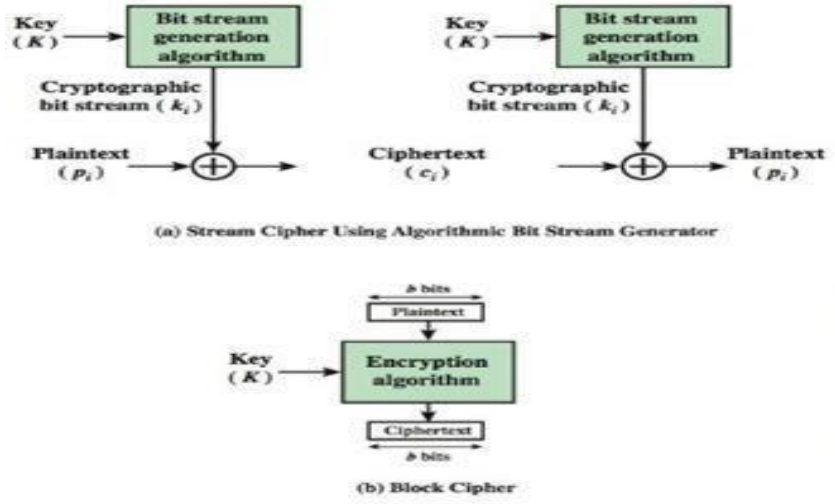


Fig 1. Stream Cipher and Block Cipher [1]

Types Of Cryptography Techniques

There are two different types of cryptographic techniques

1. Symmetric-key Cryptography

Symmetric-key algorithms are faster on computers than public-key algorithms. In public-key cryptography, also called asymmetric-key cryptography, it is hard to figure out the key for encryption to the public with no problem, and everyone can send you secret messages. But public-key cryptography algorithms are very slow on computers, so they are actually used to send a shared secret, and then symmetric-key algorithms are used for everything else because they are faster [2].

There are two kinds of symmetric-key algorithms, called stream ciphers and block ciphers. Stream ciphers encrypt a message as a stream of bits one at a time. Block ciphers take blocks of bits, encrypt them singleunit.Examples of popular symmetric ciphers include Twofish, Serpent, AES (aka Rijndael), Blowfish, CAST5, RC4, TDES, and IDEA[9].

2. Asymmetric-Key Cryptography

It is easy for a user to generate a public and private key pair for encryption and decryption. The strength is in the impossibility of recovering private key from its corresponding public key. Security depends upon privacy of private key [14]. Public key algorithms does not require any secure channel for exchanging keys between the pairs. Hence it is used only to transfer a symmetrical encryption key, using which encryption and decryption is done. Public key algorithms provide key distribution security (diffiehellamn), digital signatures (DSA) and both (RSA).

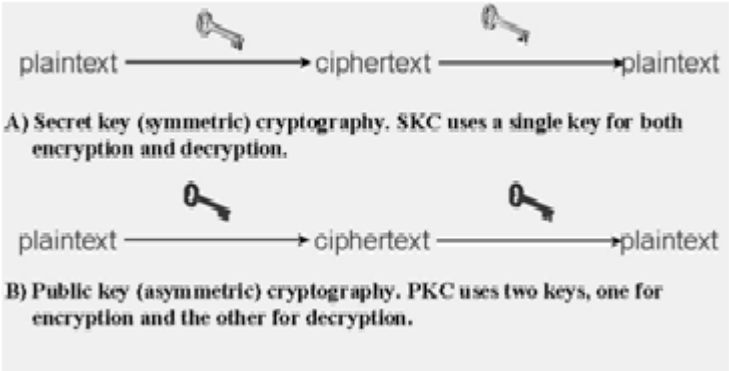


Fig 2.Symmetric and Asymmetric Cryptography

Algorithms on Symmetric Key Ciphers:

DES It uses same key for encryption and decryption of message hence both the sender and receiver know and use same private key. DES is a block cipher applied to a block of data simultaneously. To encrypt a plaintext DES group it into 64 bit blocks. By permutation and substitution each block is enciphered into a 64 bit cipher text by secret key. The process involves 16 rounds and can run in 4 different modes, encrypting blocks individually. Decryption is the inverse of encryption but reversing the order in which keys are applied [17]. For any cipher brute force attack is the basic one. It involves trying each key till finding the right answer. The length of the key determines the no of possible keys and the feasibility. DES uses a 64 bit key where 8 of those are parity checks and the rest would take maximum of 2^56 attempts to find correct key.

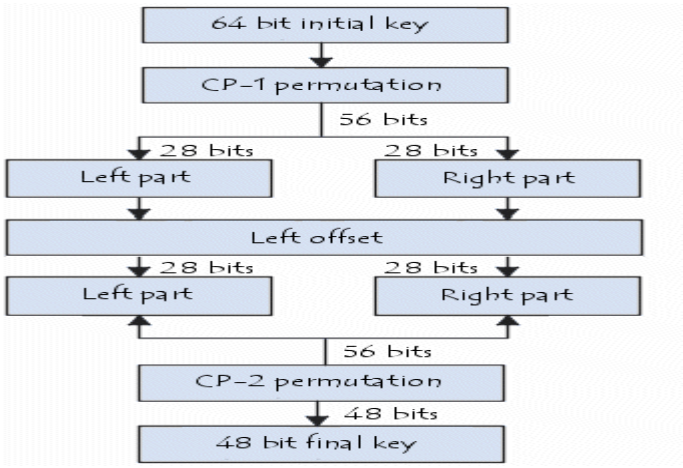


Fig 3. Data Encryption Standard

AES TheAdvanced Encryption Standard is an symmetric block cipher which is used to protect against classified information .Throughout the world it can be implemented in both hardware and software to encrypt sensitive data [18]. AES comprises of three block ciphers, they are: AES-128, AES-192 and AES-256. Using cryptographic keys of 128-, 192- and 256-bits, each cipher encrypts and decrypts data in blocks of 128 bits respectively. (Rijndael was designed to handle additional block sizes and key lengths, though its functionality was not adopted in AES)[13]. Symmetric or secret-key ciphers use the same key for encrypting and decrypting, in which both the sender and the receiver must know and uses the same secret key. All key lengths are deemed to protect classified information from "Secret" level to "Top Secret" information which requires either 192- or 256-bit key lengths. AES make use of 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys .Single round includes several processing steps they are

substitution, transposition and mixing of the input plaintext and then it is transformed to the final output of ciphertext.

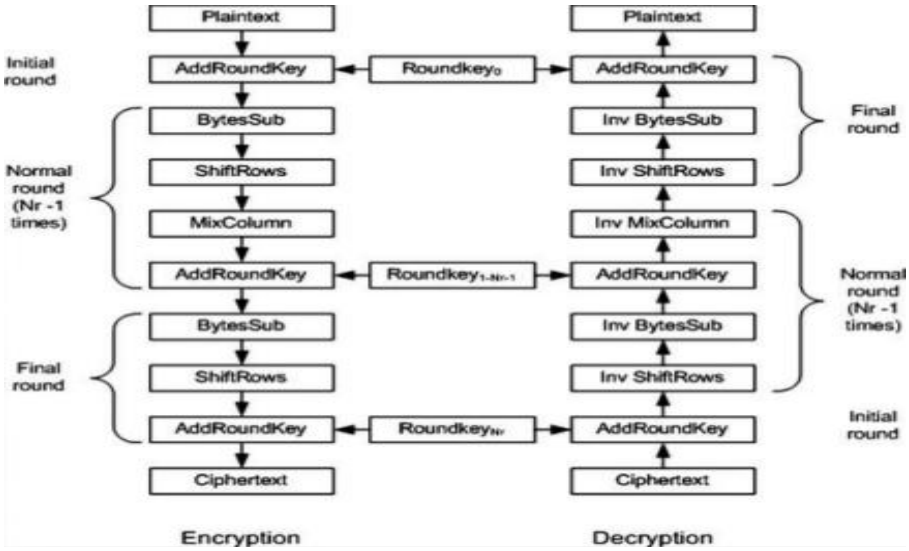


Fig 4.Advanced Encryption Standard

Blowfish: It is a kind of encryption algorithm which was used for the replacement of DES or IDEA algorithms. It is of symmetric block cipher (a secret or private key) which makes use of variable-key length, from 32 bits to 448 bits, which has been used for both domestic and exportable use [19]. (The U.S. government avoids the exportation of encryption software using keys larger than 40 bits except in special cases.) Blowfish was constructed in 1993 by Bruce Schneier it acts an alternative to existing encryption algorithms [12]. It was designed with 32-bit instruction processors in mind, which was significantly faster than DES. From its origin, it has been analyzed accordingly. Blowfish is unpatented, license-free, and available free for all uses.

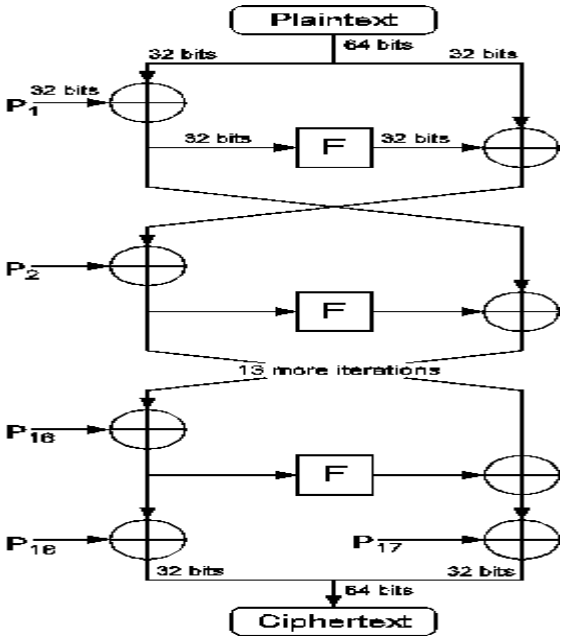


Fig 5.BlowFish

Serpent: Serpent uses symmetric key block cipher which was choosen as an finalist in the Advanced Encryption Standard (AES) contest, where it was ranked second to Rijndael.It has a block size of 128 bits

and supports a key size of 128, 192 or 256 bits.[2] Operating on a block of four 32-bit words the cipher has 32 rounds substitution permutation network and in parallel each round applies one of eight 4 bit to 4 bit S-boxes 32 times. Serpent was designed to make all operations executed in parallel, using 32 bit slices. This maximizes parallelism, which also allows to make use of extensive cryptanalysis work performed on DES[15].

Serpent took a conservative approach for security, focuses on large security margin: the designers makes use of 16 rounds to protect against known types of attack, but specified 32 rounds as insurance against future discoveries in cryptanalysis. Serpentwas designed to provide users with the highest practical level of assurance to avoid shortcut attack .To achieve this;serpent uses twice as many rounds as they are sufficient to block all currently known shortcut attacks. By using this algorithm a cipher might have a service life of a century or more.

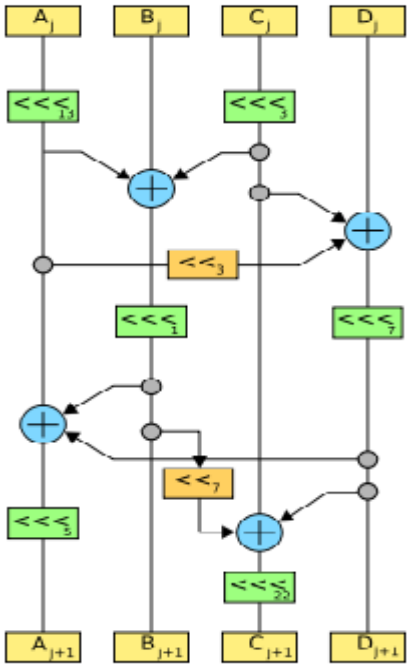


Fig 6.Serpent

Twofish: It is a symmetric key block cipher and has an block size of 128 bits and key size up to 256 bits. It was chosen as finalists in the Advanced Encryption Standard contest, though it was not selected for standardization. Twofish was slightly related with the earlier block cipher Blowfish.Twofish'sdistinctive features are used for pre-computed key-dependent S-boxes, and for a relatively complex key schedule. One half of an n-bit key is used as the actual encryption key and the other half of the n-bit key is used to modify the encryption algorithm [20].Twofish follows an Feistel structure like DES. Almost in software platforms Twofish was slightly slower than Rijndael (the chosen algorithm for Advanced Encryption Standard) for 128-bit keys, and it is somewhat faster for 256-bit keys.Twofish which borrows some elements from other designs; for example, the pseudo-Hadamard transform (PHT) from the SAFER family of ciphers.

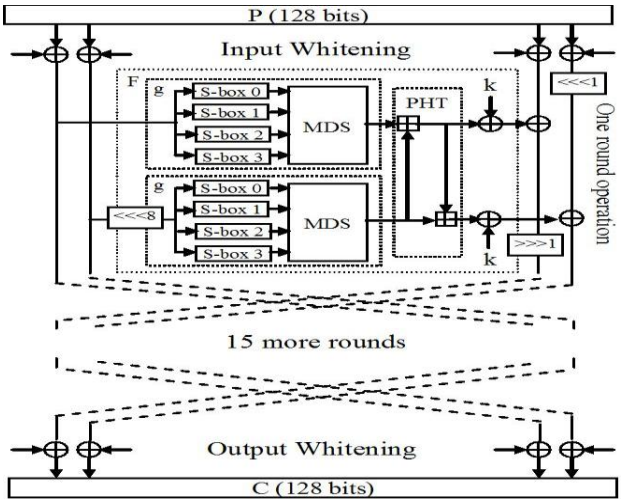


Fig 7.TwoFish

Algorithms on asymmetric key Ciphers

RSAIt is a cryptosystem for public-key encryption. When data sent over an insecure network particularly in internet, the RSA cryptosystem is used to secure the data.RSA uses public and private-key for encrypting and decrypting the data [16]. It provides confidentiality, integrity, authenticity and data storage. Many protocols like SSH, OpenPGP, S/MIME, etc uses RSA and digital signature to provide secure connection over an insecure network.

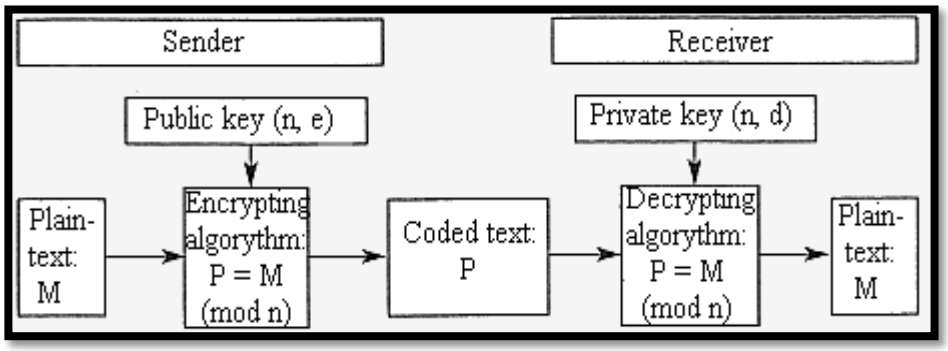


Fig 8.Rivert Shamir Adleman

Diffie Hellman Key Exchange It is a method of digital encryption also known as exponential key exchange which uses specific numbers to form decryption keys which is never directly communicated [15]. The sender and the receiver share their public keys over an internet or WAN. Both the users can generate a number x based on their own private keys [16]. The drawback of this key exchange is lack of authentication and it is prone to man in the middle attacks. Hence Diffie -Hellman should be used with any recognized authenticated method like digital signature to verify the users identity over the communication medium. It is best one for data communication but not for data storage.

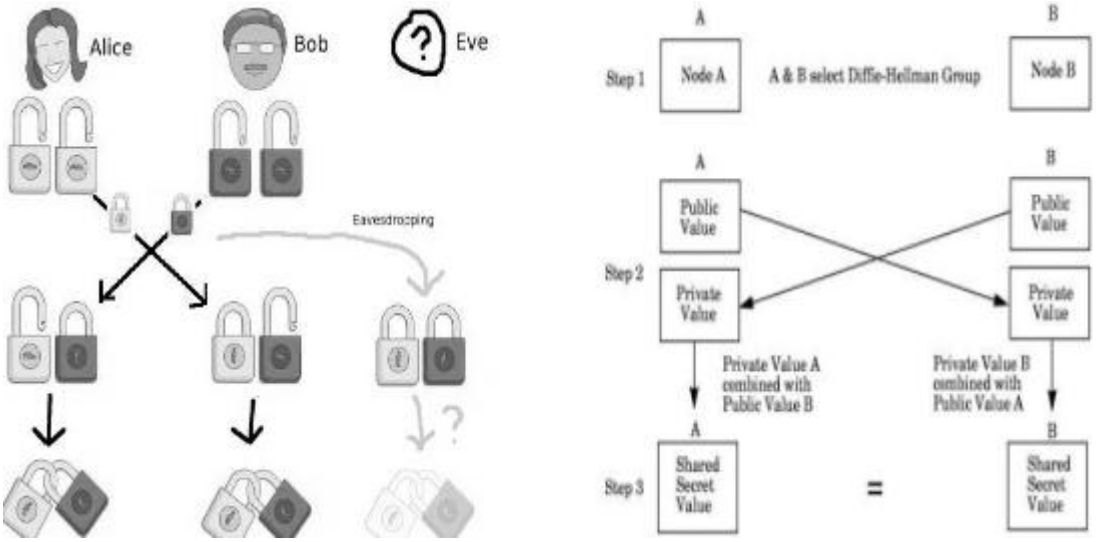


Fig 9.Diffie Hellman Key Exchange

Elliptical Curve cryptography (ECC): ECC is a public key encryption method based on elliptical curve theory which creates more efficient cryptographic keys [23]. It is used in conjunction with public key encryption methods like RSA and Diffie-Hellman. ECC can provide a level of security with a 164- bit key as it helps to establish equivalent security with lower computing power and battery resource usage while others require a 1,024 bit key[20]. ECC is based on the equation from the mathematical group derived from points where the line intersects the axes [21]. Multiplying a point on the curve by a number will produce another point on the curve, but it is very difficult to find what number was used, even if you know the original point and the result. These equations are easy to perform and very hard to reverse.

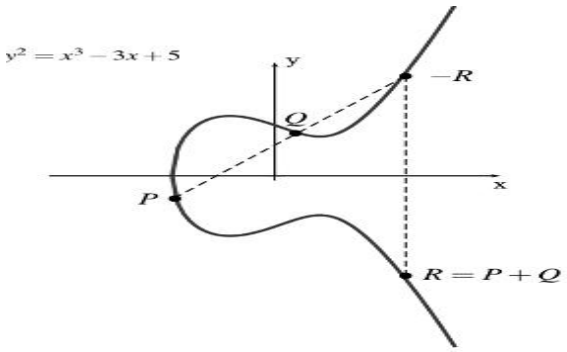


Fig 10 Elliptic Curve Cryptography

DSA: It is a pair of large numbers which are computed from specified algorithm that enables authentication of signature and provide data integrity[24]. DSA generates and verifies digital signatures. Signatures are generated by private key and verified using public key. A signature can be generated only by an authorized person using private key and verified by public key which could be used by anyone [17]. DSA generates the digital signature with the message and is verified by the same hash function.

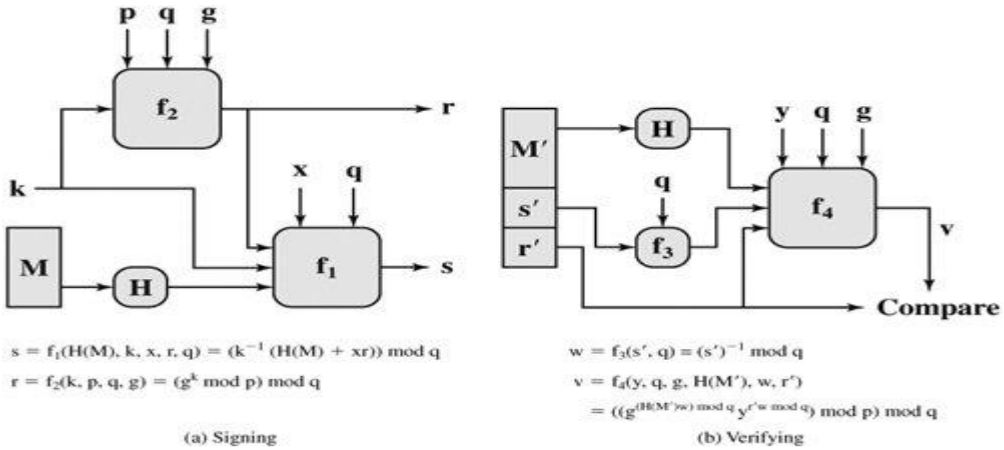


Fig 11 Digital Signature Algorithm

Modes of operations

Here we simply introduce some modes to implement block ciphers. These different modes we call them "Operation Modes" [25]. We choose one of them to implement the block cipher by considering the different kind of outstanding threatens.

ECB (electronic codebook mode) In ECB mode the encryption and decryption of the data blocks are processed independent of each other [11]. It is very fast since the operations have parallel inputs and parallel outputs. The advantage of ECB is the transmission errors could occur in single block rather than all blocks. Its drawback is the same plain text input will have the same cipher text output as the attacker could guess the data.

.

CBC (cipher block chaining mode) It overcomes the problem of ECB. The encryption is done by XOR between current plain text and former plain text, and then the result is processed with key. The output so formed is the current cipher. Decryption is done by using specification of XOR [15]. The disadvantage of CBC is the processing speed is slower than ECB as the parallel inputs could not be used

CFB (cipher feedback mode)CFB solves the problem in CBC. It can process any data that are smaller than the block size too [8]. In this the former cipher text is put into a shift register (register shifts data from left to right) and the date inside the register would be encrypted with key. The output of the encryption of left n bits is same the cipher text. The decryption is same as former modes using XOR.

CTR (counter mode or SIC) TheCTR mode uses counter to do encryption where the counter gets incremented by after each encryption [25]. The advantage of CTR is that the parallel inputs can be used hence the processing speed is faster. In this there will be no security problem happened in ECB mode. This mode is popular nowadays which is also suitable for multi-processor machine. The concept of CTR mode is familiar to OFB where register is used inside the CTR system.

OFB (output feedback mode)OFB is similar to CFB as both the modes are used transfer block cipher into stream cipher [8]. The difference between them is that OFB put the output of encryption directly into register. Hence it is simpler than CFB.

Attacks on Cryptographic Techniques

When massive computational power become available, such as grid computing, or by using cheap specialised hardware such as FPGAs, brute force attacks are possible. Another general idea of cryptanalysis is to detect and to structure the relationship between plaintext inputs, the key used and the ciphertext outputs [18].The general idea of cryptographic system is to make the plaintext to ciphertextby mapping it in random manner. But sometimes, using an attack by approximation, we can detect a structural relationship in the operation of an algorithm, which exists with some small bias (i.e., an apparent deviation from randomness).Some schemes are based on the assumed computational difficulty for solving instances of particular combinatorial problems (e.g., knapsacks, perceptron problems, syndrome decoding). Solving such problems may not so hard. As NP-complete is about the worst case, cryptography only focuses more about the average case. Cryptography is based on the factorisation which is really hard. Users can also attack the implementation. Mathematical functions simply map inputs to outputs and exist in some conceptual space, for that when we have to implement a function, where the computation consumes some resources like time and power. Encrypting data with different keys may take different time for computing. The key and the data involved affect the time taken by the users to encrypt or decrypt the message, which gives a leakage of information about the key. Even monitoring power consumption may reveal the instructions that are being executed incidentally.

Table 1: Comparison of Symmetric Key Ciphers

Factors	DES	AES	BLOWFISH	SERPENT	TWOFISH
Cipher Type	Block Cipher	Block Cipher	Block Cipher	Block Cipher	Block Cipher
Mechanism Used	Feistal Function	Substitution Permutation	Substitution Block Function	Fiestal Function	Feistal Function
Modes Of Operation	ECB,CBC	ECB,CBC	ECB,CBC	ECB,CBC	ECB,CBC
Key Length	56 bits	128 to 256 Bits	128,192 or 256 bits	32 to 448 Bits	128 to 256 Bits
Rounds	16	32	10,12,14	16	16
Security Level	Low	High	Very Low	Low	Low
Defends Against Attack	Chosen Plaintext Attack	XSL Attack	Side Channel Attack	Dictionary Attack	Impossible Differential Attack
Time Complexity	High	Low	Low	High	High

Table 2: Comparison of Asymmetric Key Algorithm

Factors	RSA	Diffie Hellman	ECC	DSA
Cipher Type	Block Cipher	Stream & Block Cipher	Stream & Block Cipher	Stream & Block Cipher
Mechanism Used	Discrete Logarithm	Modulus Exponential	Discrete Logarithm	Hash Function
Modes Of Operation	ECB,CBC	ECB,CBC,CFB, OFB,CTR	ECB,CBC,CFB, OFB,CTR	ECB,CBC,CFB, OFB,CTR
Key Length	80,1024 bits	3072 bits	80,1024,160 bits	1024,160 bits
Rounds	1	2	-	-
Security Level	High	Very Low	Very High	Low
Defends Against Attack	Cycle Attack	Man in the middle Attack	Not Prone to Attack	Key Only Attack
Time Complexity	Low	High	Low	High

Conclusion

This paper gives a complete survey on Elementary, Symmetric and Asymmetric cryptographic systems techniques that are very effective in securing the messages over any communication medium. Also it thoroughly gives an analysis of different symmetric and asymmetric cryptographic techniques. Various characteristics of the different cryptographic techniques have been compared and results have been tabulated. Thus the paper gives an idea of defending against attacks using the symmetric and asymmetric cryptographic techniques

References

[1]www.cyberrights.org
[2]www.csprinceton.org
[3]www.garykessler.net/library/crypto.html
[4]crypto.interactivemaths.com
[5]en.wikipedia.org/wiki/Symmetrickeyalgorithm
[6]en.wikipedia.org/wiki/Publickey_cryptography
[7]practicalcryptography.com
[8]sovannarith.files.wordpress.com/2012/07/cryptology.pdf
[9] www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf
[10] www.ijettcs.org/Volume3Issue4/IJETTCS-2014-08-25-137.pdf
[11] www.slideshare.net/aouyang/5-cryptography-part1-11860053
[12] www.slideshare.net/sumitlole/elementrycryptography1
[13]disp.ee.ntu.edu.tw
[14] W. Stallings, Cryptography and NetworkSecurity Principles and Practices Fourth Edition,Pearson Education, Prentice Hall, 2009. [2]
[15]Sourabh Chandra, SmitaPaira, SkSafikul Alam, GoutamSanyal ,comparative survey of symmetric and asymmetrickey cryptography 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)978-1-4799-5748-4/14/2014 IEEE .
[16]www.searchsecurity.techtarget.com/asymmetrickeyciphers
[17]ccm.net/contents/134-introduction-toencryption-with-des
[18]www.pling.org.uk
[19]www.drdobbs.com/security/the-blowfishencryption-algorithm/184409216
[20]www.windtalkers.nettwofish-encryptionalgorithm
[21]www.globlib4u.wordpress.comrsapublic-key-encryption system
[22]www.slideshare.netpublic-keycryptography
[23]www.embedded.comAn-Introductionto-Elliptic-Curve-Cryptography
[24]www.flylib.comdigitalsignaturealgorithm
[25]en.wikipedia.org/wiki/Block_cipher_modes of operation