Modern Cryptography - A Review

Seetha. R, Mythili. N

Abstract: Cryptography techniques involve message conveyance either in a secret form or in some hidden form. Cryptography finds it applications in almost all fields for secure data transfer. Looking into the history it is the military field which is very much influenced by secure data transfer and communication. Use of cryptography has spread its wings once digital communication stepped in. The thirst of data security increased when digital communication started using wireless medium for data transmission. It is therefore necessary to understand the basics and importance of cryptographic techniques for better, fast and efficient data transfer without any intrusion.

Index Terms: Encryption, Decryption, Plaintext, Cipher text, Cryptanalysis, Data security.

INTRODUCTION

The necessity of communicating and sharing information in a selective manner from one end to another end has led to the evolution of cryptography. The true security strength of cryptographic algorithms lies on the cryptanalysis which is the ability to break the encrypted (cipher) text. Thus cryptography and cryptanalysis always coexist and are collectively known as cryptology. The major focus of cryptography is to provide secure data transmission which include data confidentiality, integrity, non-repudiation, and authentication. In order to ensure security, cryptographic technique uses mathematical concepts like number theory, probability etc. The important primitive techniques that provides data security are encryption, hash function, message authentication codes and digital signature. In classical approach of cryptography characters and digits are directly manipulated and requires entire communicating environment to be a trusted and confidential one. In modern approach, binary bit sequences are used for manipulation. These bit sequences are manipulated using known mathematical algorithms with increased computational complexity thus challenging the third party from gaining information, Dan Boneh and Victor [2]. The basic and important terms in cryptography and cryptosystem includes plain text, cipher text, encryption and decryption. The plain text is the original message that is to be conveyed to the other end. The cipher text is the encrypted form of plain text which prevents unauthorized access when transmitted over the medium. The technique used for converting plain text into a cipher text is called encryption and reverse process is called decryption. The plain text is encrypted and decrypted using a secret key. Based on the key used, the cryptosystem could be classified as symmetric cryptosystem and asymmetric cryptosystem. The symmetric cryptosystem uses the same key for encrypting and decrypting the information. The asymmetric cryptosystem uses two keys namely public key and private key where one is used for encrypting the message and the other corresponding key is used for decrypting the message.

I. EVOLUTION OF CRYPTOGRAPHY

Cryptography has come into practice since 1900BC. The following table (Table 1) gives a picture of cryptography's evolution from scratch and the evolution of new cryptographic techniques still continues, Nicholas and Donald [6], Singh [5].

II. MATHEMATICAL CONCEPTS IN CRYPTOGRAPHY

In [1] Ruohonen has discussed mathematical concepts which are applied in cryptographic techniques. Mathematical concepts like but not limited to number theory concepts like divisibility, factors, primes, integer representation with different radix, GCD, LCM, modular arithmetic, rings and prime fields and basic arithmetic operations are widely used in cryptosystems and cryptanalysis. Other concepts include algebra, permutations and combinations, substitutions, complexity theory of algorithms (NP-hard and NP-complete problems), Euler's function, discrete logarithm, Chinese Remainder Theorem, Factorization, modular square root, random numbers, lattices, exponentiation, groups, elliptic curves, vectorization and quantum theory. Table 2 below summarizes few of the mathematical concepts applied in cryptographic techniques

III. TYPICAL CRYPTOGRAPHIC ALGORITHMS

The following algorithms discussed are one that are used in ancient days for secure data transmission and are symmetric key techniques, DR Stinson [4]. Caesar cipher: Caesar cipher is a simple and a type of substitution cipher. It is also known as shift cipher. This method was used by Julius Caesar for communicating and hence named after him. The idea behind this technique is each character in the plaintext is shifted a certain number of places down the alphabet.

Table 1: Evolution of Cryptography

Year	Techniques used
1900BC	Evidence shows cipher text (Jumble letters) was carved on a stone in Egypt
1500BC	In Mesopotamia information to be secured are written on clay slabs
500BC	Spartans used Scytale device for sending and receiving secret messages. Scytale used transposition cipher.
400BC	Karma Sutra
800AD	Frequency analysis technique was used for breaking mono alphabetic ciphers
1467AD	Poly alphabetic ciphers was used
1400s-1600s	Cryptography used for political and religious issues.
1853-1856	Charles Babbage used Vigenere cipher
1854	Playfair cipher was invented by Charles Wheatstone. It was used upto Worldwar II.
1917	Gilbert Vernam devised a telerpinter cipher
1920s-1930s	Enigma rotor machine (German) was introduced and later its performance was improved using Typex machine (British) and SIGABA machine (US).
1942	JN-25 Japanese Navy Cryptosystem was broken by US navy
1950s	VIC cipher was discovered
1975	DES was established for secure electronic communication in financial organizations
1976	Diffe-Hellman key exchange was introduced

1991	PGP (Pretty Good Privacy) was released
2001	AES came into use

For example, with a shift of 2, A would be replaced by C, B would become D, and so on. As per cryptanalysis Caesar cipher could be easily broken Simple substitution cipher: This method can be called as an optimization form of Caesar cipher. The characters in the plain text are not shifted rather some permutation in other words jumbled set of alphabets are applied to it. The permutation chosen is used as the secret key. Hence with 26 letters in alphabet, the possible permutations are 26! (Factorial of 26). The sender and the receiver may choose any one of these possible permutation as a cipher text alphabet. Though the possible number of permutation used in this

Table 2: *Mathematical concepts in cryptosystems*

Mathematical concepts	Application in cryptography
Number theory	Applied in public key cryptography and error correcting codes.
Primes	Plays vital role for security of encryption algorithm and is based on the multiplication of two large prime numbers.
Factorization	RSA, Shor's algorithm, Pollard's ρ algorithm, Sieve algorithm.
Random numbers	Pollard's ρ algorithm, key generation algorithms, nonce, salts in signature algorithm like ECDSA, RSASSA-PSS, block cipher, stream cipher.
Substitution	Simple substitution cipher algorithm, homophonic, polyalphabetic, polygraphic, one-time pad, and nomenclator.
GCD (Greatest Common Divisor)	RSA, Stein's algorithm
Discrete Logarithm	El-Gamal encryption for key generation, Diffie-Hellman key exchange, Digital Signature algorithm.
Chinese Remainder Theorem	Mignotte's Threshold secret sharing scheme, Asmuth-Bloom Threshold secret sharing scheme, RSA-CRT for faster decryption.
Modular Arithmetic	Vignere cipher, RSA, Diffie- Hellman key exchange, El-Gamal algorithm.
Exponentiation	Public key cryptosystems, Signature algorithms, public key distribution schemes.

Technique is large the design is simple and could be broken when permutation chosen is weak. Mono alphabetic cipher: Mono alphabetic cipher means a single character in plain text is replaced with a single character in cipher text irrespective of number of occurrences of characters in plain text. As an example if A is replaced with X then whenever A occurs in the plain text it is substituted with X for the cipher text and thus have a weaker part of cryptanalysis. Caesar cipher and Simple substitution cipher are examples of mono alphabetic cipher. Polyalphabetic cipher: Polyalphabetic Cipher is also a type of substitution cipher. As the name indicates multiple character are used to replace a single letter in a given plain text. Thus the cipher text will have different characters substituted for repeated characters in plain text. Examples of polyalphabetic cipher include playfair and Vigenere Cipher. Playfair cipher: This symmetric key encryption is the first graphical substitution cipher. In this technique pairs of letters are encrypted instead of single letter. The Playfair cipher uses a key table where the key is arranged as a 5*5 grid. Only 25 alphabets are used as 'J' is omitted. If occurs on the plain te xt it is replaced with 'I'. The key is arranged row by row with duplicates removed and rest of the space is filled with remaining letters in the alphabet. Frequency analysis is also possible on the Playfair cipher, however it would be against 600 possible pairs of letters instead of 26 different possible letters. Thus the Playfair cipher is much more secure than other substitution ciphers. Steps given below explains the process carried out in Playfair cipher.

- First, a plaintext message is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.
- Rules for encryption:
  - If both the letters are in the same column, take the letter below each one (going back to the top if at the bottom).
  - If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right).
  - If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

Vigenere cipher: This polyalphabetic cipher technique uses a 26×26 table with A to Z as the row heading and column heading and referred to as the Vigenère Table or Vigenère Square. The first row of this table has the 26 English letters. Starting with the second row, each row has the letters shifted to the left one position in a cyclic way. For example, when 'B' is shifted to the first position on the second row, the letter 'A' moves to the end. The size of the symmetric key used should be equal or less than the size of the plain text to be transmitted. The encryption process at various stages of the cipher uses a different character from one of the rows. The character used at each point depends on a repeating keyword. This cipher technique is called as unbreakable cipher and has been used for three centuries transferring highly confidential data. One-time pad: It is a variant of Vigenere cipher. The symmetric key of one time pad is used only once and is of same length or more than the size of the plain text. The key is a string which is generated randomly. One time pad provides perfect secrecy provided

- Key used is truly random and is of same size of the plaintext.
- Key is never reused in whole or in part and kept completely secret.

Transposition cipher: In this technique the plain text is encrypted by shifting the characters or by messing up or jumbling the characters of plain text. One such transposition cipher is a simple columnar transposition cipher where the plaintext is written horizontally row by row. The number of columns for representing plain text is equal to the size of the key used. Then the cipher text is written by reading the

characters vertically. For decryption, similar table is created by the receiver. The number of rows is obtained by dividing number of total cipher text alphabets by key value (integer division is performed). The receiver then writes the received cipher text vertically down and from left to right column. To obtain the original plain text the table is read horizontally left to right (row by row). Cryptanalysis is challengeable when the key used is considerably long. Table 3 below summarizes briefly about typical cryptosystems.

Table 3: Summary of Typical Cryptosystem

Cipher	Encryption process	Cryptanalysis
Caesar cipher	Mono alphabetic substitution	Easily breakable
Simple substitution cipher	Uses permutations of 26!	Secure than Caesar cipher
Playfair cipher	Poly alphabetic substitution	Secure than mono alphabetic
Vigenere cipher	Uses 26*26 Vigenere table	Secure
One time pad	Uses the key only once and is generated randomly	Perfect secrecy
Transposition cipher	No substitution rather shifts the characters of plain text	Secure when size of the key used is long

IV. MODERN CRYPTOGRAPHIC ALGORITHMS

This section gives a description of shared secret key, private and public key algorithms, its security nature and applications. Symmetric key algorithms: The word 'symmetric' means 'an agreement'. The persons involving in communication agree upon a common private key which is shared among them and is only known to them (sender and receiver). This shared secret key is used for encrypting and decrypting messages. The strength of symmetric key encryption lies purely on the secrecy of common shared key. Basically symmetric encryption is of two types: block and stream. In block type the data bits are encrypted using the shared secret key as blocks of specific size. As the data is being encrypted, the system holds the data in its memory as it waits for complete blocks. In stream type data is encrypted as streams and not retained in the memory. AES (Advanced Encryption Standard), DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfish (Drop-in replacement for DES or IDEA), RC4 (Rivest Cipher 4), RC5 (Rivest Cipher 5), RC6 (Rivest Cipher 6) are some of the symmetric key algorithms. AES, DES, IDEA, Blowfish, RC5 and RC6 are block ciphers. RC4 is stream cipher. DES (Data Encryption Standard) is the first symmetric key encryption algorithm came into use in 1977, Thakur [17]. It is no longer used due to high processing power of today's processors. Depending on the key used DES could be 2-DES or 3-DES. Though DES is considered insecure 3-DES is still being used in EMV (Europay Mastercard and Visa) chip cards. AES (Advanced Encryption Standard), initially known as Rijndael [18] is highly secure than DES. AES is an approved standard of the U.S. National Institute of Standards and Technology (NIST) in 2001 for encrypting the electronic data announced in U.S. FIPS PUB 197. Under NIST, the AES cipher has a block size of 128 bits, but can have three different key lengths as shown with AES-128, AES-192 and AES-256. AES-128, AES-192 and AES-256 are the most widely used symmetric key algorithms. AES has less computational power and is considerably faster. Most VPN (Virtual Private Network) services use AES-256 to secure data transmitted by the OpenVPN protocol. IDEA algorithm is originally called as Improved Proposed Encryption Standard (IPES) and proposed as a replacement for DES algorithm, Leong [19]. The data are encrypted as 64 bit blocks using 128 bit key. It is used in Pretty Good Privacy (PGP-v2). IDEA finds its applications in financial services, broadcasting. The IDEA algorithm is adaptable and could be used to protect data transmission and storage. Few areas where IDEA is employed include transmission of audio and video data for cable television, video conferencing, distance education, confidential and commercial data services and smart cards. Blow fish algorithm developed by Bruce Schneier [16] in 1993 is fast and an alternate encryption algorithm for DES or IDEA. It is a 64-bit block cipher and uses a variable length key ranging from 32-448 bits. It could be used for all public purposes as it is available for free. It is used in a product called splashID which is used in processors of mobile phones, desktop and notebook systems. RC4 developed by Ronald Rivest, Charbatia and Sharma [20] is a stream cipher encryption algorithm. It is used by IEEE 802.11 within WEP (Wireless Encryption Protocol) using 40 and 128-bit keys. It is simple and 10 times faster than DES but it is no longer used as it is considered to have weak keys. RC5, Rivest [21] called as 'Rivest Cipher' is a block cipher developed in 1994. It is used for both software and hardware implementations. It is simple, fast and adaptable to processors of any word length. The structure of the algorithm is iterative and uses a variable length key. The number of iterations depends on the size of the data used for encryption and hence not predetermined. It is used for secure transmission of digital images. RC6 an extension work of RC5, Rivest et al. [22] is simple, compact, secure and offers good performance. RC6 is a variable block size, a variable key size, and a variable number of rounds algorithm which has been designed to meet the requirements of AES. The difference between RC5 and RC6 is that in RC5 two working registers are used but in RC6 four registers are used and additionally in RC6 integer multiplication is included thus increasing security and throughput of each iterations of encryption process. RC6 is faster than RC5. RC6 is used for applications like e-commerce, mobile networks, bank ATMs, transferring digital images, military applications and transmission of audio and video data. Table 4 summarizes the concepts of symmetric key algorithms discussed. Asymmetric key algorithms: Asymmetric key encryption commonly called as public key encryption uses two keys: private key and public key. The private key is kept secret and public key is shared. Either of the key could be used for encryption and subsequently the other key will be used for decryption. The difference between Symmetric and Asymmetric Encryption

- In symmetric encryption sender and receiver uses a single shared key for encryption and decryption. In asymmetric encryption a pair of public key and a private key is used for encrypting and decrypting messages.
- Symmetric encryption is an old technique while asymmetric encryption is relatively new.
- Symmetric encryption is faster than asymmetric encryption.

The basic part of asymmetric encryption is to eliminate the

concept of single shared key that is used for encrypting and decrypting messages. Examples of public key encryption includes RSA, Diffie-Hellman key exchange and Digital Signature algorithms. The public key encryption algorithms are based on number theory concepts like discrete logarithms, large prime numbers, and Chinese remainder theorem. The highlights of public key encryption is that It is computationally easy to generate a pair of public key and private key, to generate a cipher text using the public key, to decrypt the cipher text using the private key but it is computationally infeasible to determine the private key from the public key and to recover the message from the cipher text and the public key. Burnett, Steve and Stephen [7] in their book about RSA has discussed that RSA public key encryption algorithm proposed in 1977 is named after its authors R-Rivest, S-Shamir and A-Adleman. It is the most widely used algorithm for secure transmission of data. RSA uses public key for encryption and private key for decryption. The computational complexity of RSA is based on the factorization of product of two large prime numbers used. The user who wishes to send a secure message using RSA creates a public key by choosing two large prime numbers. These prime numbers are kept secret. The public key along with an auxiliary value is published. This public key is used for encryption and private key is used for decrypting the message. Hence the user with the knowledge of prime numbers used alone could easily decrypt the message. But on the other side RSA is assumed to be relatively slow compared to symmetric key encryption and hence RSA is used to share the secret key of symmetric encryption. RSA is used for securing communications between web browsers and e-commerce websites. It is also used in Bluetooth applications, Master cards, VISA cards and e-banking. Diffie-Hellman key exchange algorithm published in 1976 is released by Diffie and Hellman [9] but it is originally abstracted by Ralph Merkle. This key exchange algorithm allows any two parties unknown of each other to generate a secret key over insecure medium. This key could be used to share the symmetric secret key, it is being used for many e-services and for authentication purposes. Diffie-Hellman key exchange is also called as exponential key exchange algorithm and offers perfect forward secrecy. It is actually a key agreement protocol where users don't exchange the key but jointly derives the key. The security of this algorithm is based on the computational complexity of discrete logarithm problem. When two users wants to communicate with each other, they first agree upon on a large prime number p, and a generator (or base) g (where $0 < g < p$).Then user A computes the public key g^a mod p where 'a' is the secret value of user A. Similarly user B computes his/her own public key g^b mod p where 'b' is the secret value of user B. Now these public key is shared among them and thus b is unknown to user A and a is unknown to user B. Using this public key user A and B creates a common key $(g^b \bmod p)^a$ mod p and $(g^a \bmod p)^b$ mod p respectively. Thus user A and B have derived their common secret key. 'Digital Signature', as the name indicates it is the way of verifying and validating the authenticity of digital documents and messages cryptographically. It is similar to MAC (Message Authentication Code) with a difference that MAC is symmetric and digital signature is asymmetric. The sender who signs the message digitally uses the private key for encrypting the signature and its related data. The authenticity and integrity of the digital signature is verified by the receiver by decrypting it using its public key. Digital Signatures provide authentication, integrity and non-repudiation and hence they are widely used in confidential, financial and commercial services and applications. Moreover digital signature cannot be forged and reused. Examples of digital signature algorithm include ElGamal, DSA, Schnorr, RSA, Rabin and Nyberg-Rueppel. In case of ElGamal, DSA, and Schnorr the original message is required for verifying the digital signature and it uses hash functions. Whereas in RSA, Rabin and Nyberg-Rueppel the original message is retrieved from the signature itself. The ElGamal [10] algorithm is based on computation complexity of discrete logarithm problem. It is applied in e-mail applications, secure use of digital library and other internet services. DSA (Digital Signature Algorithm) is a Digital Signature Standard (DSS) introduced in 1991. The National Institute of Standards and Technology (NIST) issued the standard in 1994. The standard DSA is preferred worldwide for signing e-documents digitally as that of RSA for creating digital signatures. Most of the digital signature algorithms generate signature by signing message digests with the private key of the owner and claims that the signature is smaller compared to the data that was signed and hence impose less load on processors for signature verification. But DSA, does not encrypt message digests. DSA generates two 160 bit numbers from the message digest and private key. Then it applies mathematical functions to create a digital signature. The signature is verified for authenticity using public key, Abhishek and Sunil [28]. DSS (Digital Signature Standard) developed by the U.S. National Security Agency, is a collection of procedures and standards for generating a digital signature and has become the U.S. government standard for authenticating electronic documents. DSS ensures all the properties of digital signature such as authentication, integrity and non-repudiation and hence it is used in e-fund transfer services, e-software distribution and storage applications. DSS is adaptable to hardware, software and firmware. The algorithm used behind the Digital Signature Standard is known as the Digital Signature Algorithm. The digital signatures are generated by the originator using private key and verifiers verify the signature using public key. The highlight part of encryption and signature operation in the Digital Signature Standard is that encryption is reversible, whereas the digital signature operation is not. The other important point to be noted is that the security of the digital signature standard depends on the secrecy of private key of the signer. Schnorr digital signature algorithm proposed by Claus Schnorr [13] is simple and is based on discrete logarithm problem. It is an efficient scheme and generates short signatures which is of 64 bytes in size. The digital signature generation process could be done in idle time. Schnorr allows to combine multiple signatures into one single Schnorr signature of 64 bytes and thus it could be used for multi-signature transactions. Schnorr signature is employed nowadays in bitcoin applications and block chain technology. In [8], Rivest has discussed about RSA digital signature which generates digital signature using RSA public key encryption algorithm. The signature is generated by applying the originator's private key on the message and verified using corresponding public key. RSA signature is generated by applying a cryptographic hash function (SHA) to the message. The hash function applied to the message of any length

produces a hash value of 160 bits. The key points of hash value is that it is difficult to find a message with a specific hash value and it is difficult to find two messages with the same hash value. As a next step the hash value is converted to a "message representative" which is an integer. The message representative is of same length of the private key used which is done by applying a padding format to the resulting hash value. The use of padding format ensures additional security. Finally the digital signature is generated by employing primitive values to the message representative using private key of the originator. Rabin digital signature algorithm developed by Michael Oser Rabin [11] in 1979 is based on the strength of integer factorization. Like RSA digital signature, Rabin is also probabilistic and the procedure is also similar to RSA. The difference is that Rabin signature uses small exponent and the signature verification process is faster than RSA. Nyberg-Rueppel [12] Signature algorithm proposed in 1995 is based on discrete logarithm problem. The main aim of this algorithm is to show that the message and signature are independent. No hashing function is employed on the message rather message is recovered from the signature at the verifier's end. The other key points include generation of small signatures for small messages and could be integrated with other signature schemes like ElGamal. The signer uses the private key for generating the signature and function inversion process.

Hashing functions in Cryptography: Hash function is a mathematical function which takes input of varying length and produces output of fixed size. The output value obtained is called hash value or message digest. Thus the process of hashing is application of a mathematical hash function to an input value to produce a hash value of fixed length. Hash functions could also be called as compression functions as the hash value produced is smaller than the input size. Usually hash values will be of 160 bits-512 bits. The key point of hash function is that it is computationally fast and computationally hard to reverse that is hash function is one way. Hash function applied on different inputs produces different hash values. Hashing is widely used in password storage and retrieval, it is used to check integrity of data stored and for efficient search of data. To name a few: Message Digest (MD) hash function, Secure Hash Function (SHA), RACE Integrity Primitives Evaluation Message Digest (RIPMED) hash function, BLAKE2, Whirlpool. The variants of MD hash function are MD2, MD4, MD5 and MD6. Among these MD5 is used widely. MD5 hash function proposed by Rivest [24] produces a 128 bit hash value and is applied for integrity check of files stored. Using MD5 a check sum is computed for the files stored by the file server. Whenever the file is downloaded the computed checksum value is compared with the precomputed one to check its integrity. But on the other hand MD5 is found to be non collision resistant function.SHA variants include: SHA-0, SHA-1, SHA-2, and SHA-3. SHA-0 produces 120-bit hash values. SHA-1 produces 160-bit hash values and its operation is similar to MD5 (early version). It has cryptographic weakness and is not recommended for use since the year 2010. SHA-2 has two hash functions: SHA-256 and SHA-512. SHA-256 uses 32-bit words. SHA-512 uses 64-bit words. SHA-3 earlier called as Keccak. Among these SHA-1 is widely used and it is used in applications of Secure Socket Layer (SSL). SHA-1 is also not collision resistant and it is not being employed since 2010, Gupta and Kumar [25]. SHA-2 is strong but uses design principles of SHA-1. SHA3 is said to offer good and efficient performance.The most popular and secure RIPEMD hash function is RIPEMD-160, Dobbertin et al. [26] and the other variants are RIPEMD, RIPEMD-128, RIPEMD-256, and RIPEMD-320. RIPEMD functions are applied in Bitcoin applications. It uses the design principles of MD4, Dobbertin [23]. RIPEMD-160 is used in applications that require shorter hash value. BLAKE2, Aumasson [27] is a cryptographic hash function which is widely being employed in many applications as it is simple, secure and faster than other hash functions. The variants of BLAKE are BLAKE-256, BLAKE-224, BLAKE-512 and BLAKE-384. BLAKE-256 and BLAKE-224 use 32-bit words and produce digest sizes of 256 bits and 224 bits, respectively, while BLAKE-512 and BLAKE-384 use 64-bit words and produce digest sizes of 512 bits and 384 bits, respectively.

Whirlpool hash function proposed by Baretto and Rijmen [3] is an open and scalable cryptographic function which produces a message digest of 512-bit. It is a block cipher based hash function and is based on the design principles of AES encryption.

Table 4: Summary of Symmetric key algorithms

Hash functions	Variants	Rounds	Hash value (bits)	Security
MD	MD2 MD4 MD5 MD6	18 3 64 Varies	128 128 128 0-512	Non collision resistant
SHA	SHA-0 SHA-1 SHA-2 (256/512) SHA-3	80 80 64/80 24	160 160 256/ 512 1600	SHA-2 is secure
RIPEMD	RIPEMD RIPEMD128 RIPEMD160 RIPEMD256RIPEMD320	48 64 80 64 80	128 128 160 256 320	RIPEMD-160 is widely used and secure
BLAKE	BLAKE2s BLAKE2b	10 12	256 512	Secure and fast
WHIRLPOOL	Whirlpool Whirlpool-0 Whirlpool-T	10	512	Secure

Whirlpool is available in three variants: Whirlpool, Whirlpool-0, and Whirlpool-T. It is a one-way collision resistant function comprising iterated application of compression function. Whirlpool requires much less storage space and it is being applied in smart card security applications. Table 5 summarizes about hash functions discussed.

Table 5: *Comparison of hash functions*

Symmetric key algorithms	Block/ Stream	Key/Encryption process/Structure	Security
DES	Block	56 bit key / 16 rounds/ Balanced Feistel network	Weak
AES	Block	128 bit key/10 rounds/ Substitution–permutation network	Strong and still recommended
IDEA	Block	128 bit key/ 8.5 rounds/ Lai-Massey scheme	Averagely secure and being used for commercial purposes
Blowfish	Block	32-448 bit key/ 16 rounds/ Feistel network	Secure and used for commercial purposes
RC4	Stream	40–2048 bits key/ 1 round	Weak
RC5	Block	0 to 2040 bits key(128 suggested)/ 1-255 rounds (12 suggested originally)/ Feistel-like network	Secure and used in digital image transmissions.
RC6	Block	128, 192, or 256 key bits/ 20 rounds/ Feistel network (Type 2)	Highly secure and good performance.

V. TRENDING CRYPTOGRAPHIC ALGORITHMS

Modern approach to security uses algorithms like elliptic curve cryptography, quantum cryptography and are considered to be secure for deploying in various application. Elliptic Curve Cryptography (ECC): Lauter and Kristin [14] discussed about the advantages of elliptic curve cryptography for wireless security. The elliptic curve cryptography is based on elliptic curve theory over finite fields. It is a public key encryption technique capable of establishing small and efficient keys at faster rate. ECC provides a high level security with164-bit key while other algorithms require 1,024-bit key. ECC is used in many mobile applications as it has low computing power and consumes less battery usage. ECC follows the same design principles of RSA and Diffie-Hellman algorithms with a difference that the primes numbers used in the computation are chosen from a finite field defined within an elliptic curve expression. ECC uses an elliptic curve equation obtained from points where the line intersects the axes. Multiplying a point on the curve by a number will produce another point on the curve. This number cannot be determined even if the original point chosen and the result value is known. The equations based on elliptic curves are relatively easy to perform and extremely difficult to reverse. Quantum cryptography: Quantum cryptography dates back to 1970s and first proposed by Stephen Weisner in his work “Conjugate Coding”. It is based on physics whereas other cryptographic algorithms are designed based on mathematical concepts. Quantum cryptography is based on the behaviour of individual particles/waves of light (photon) and their intrinsic quantum properties. The algorithms developed using quantum are considered to secure and unbreakable as it is impossible to measure the quantum state of any system without disturbing that system. This method of cryptography provides a secure way distributing shared secret key among the users for encryption and decryption purposes. Quantum computation is performed in a quantum computer or processor which stores data using a quantum superposition of multiple states. These multiple valued states are stored in "quantum bits" or "qubits." The quantum cryptography is expensive and still it is in development stage, Hughes et al. [15]. Though elliptic curve and quantum cryptography provides high security for data transmission they are not fully deployed and has a very long way to go and hence could be called as forthcoming cryptographic techniques.

VI. CRYPTANALYSIS TECHNIQUES

Cryptanalysis is study of cipher text which is carried out either to weaken the security of process carried out or to improve the strength of process for better security and to make it error free technique. The commonly used cryptanalytic techniques include, William Stallings [29]:Cipher text-only attack: As the name indicates the attacker has only cipher text in hand but has no knowledge about plain key and the encryption process. The attacker with a collection of cipher text analyse it to gain some knowledge about the process applied over and tries to determine the secret key used to recover the plaintext. Known plaintext attack: In this type if attack the analyst may have access to some or all of the plaintext of the cipher text and tries to discover the key used for encryption and decryption. Once the key is discovered, all the cipher text could be decrypted and the plain text could be accessed. Linear cryptanalysis is a type of known plaintext attack. Chosen-Plaintext attack: A cryptanalyst with access to plaintext data tries to gain the secret key or alternatively use an algorithm for decrypting any cipher text messages encrypted using the key even without the knowledge of the key. Chosen-cipher text attack: In this attack a cryptanalyst analyses any chosen cipher text together with its corresponding plaintext and tries to gain knowledge about the secret key applied or tries to get as many information about the attacked system as possible. Chosen-key attack: The aim of this attack is to weaken the entire encryption process carried out. Brute-Force attack: It is also called as exhaustive key search in which all possible keys are applied to gain access to the plain text. Dictionary attack is a kind of brute-force attack. DoS attack: Denial of Service (DoS) attack is one in which the attacker interrupts the services of the host and hence prevents other users from accessing the resources. Man-in-the-Middle attack: Man in the middle is an intruder whose presence is hidden from the communicating parties and tries to take part in the communication without their knowledge. The intruder gains access to the communication by sharing his secret keys with the communicating parties (uses two keys one for each party) and hence gathers information.

VII. SUMMARY

A complete review of commonly used cryptographic techniques are discussed along with its pros and cons and area of applications. The review presented here are from scratch and till future. It is clearly understood that the computational complexity of mathematical concepts rules the current world of cryptography but a shift to other area may

happen in few decades or centuries. But the true strength of these techniques really lies on its ability to withstand any type of cryptanalysis done on it. In this digital era data are transmitted over insecure wireless medium. To secure these data the study clearly narrates the importance of cryptography in view of data authentication, integrity and confidentiality.

REFERENCES

[1] Ruohonen,Keijo. Mathematical cryptology. LectureNotes, 2010, pp.1-138.

[2] Boneh, Dan, Victor Shoup. A graduate course in applied cryptography, Draft 0.2, 2015.

[3] Barreto, P. S. L. M., Vincent Rijmen. The Whirlpool hashing function. First open NESSIE Workshop, Leuven, Belgiu, Vol. 13, 2000, pp.14.

[4] Stinson, Douglas R. Cryptography: theory and practice. Chapman and Hall/CRC, 2005.

[5] Singh S. The code book: the science of secrecy from ancient Egypt to quantum cryptography, Anchor, 2000.

[6] Nicholas GM, McDonald G. Past, present, and future methods of cryptography and data encryption. Department of Electrical and Computer Engineering University of Utah. 2015.

[7] Burnett, Steve, Stephen Paine. The RSA security's official guide to cryptography. McGraw-Hill, Inc., 2001.

[8] R. Rivest, A. Shamir, L. Adleman. A method for obtaining digital signatures and public-key cryptosystems, ACM, Vol 21, 1978, No 2, pp. 120–126.

[9] Diffie, Whitfield, Martin Hellman. New directions in cryptography, IEEE transactions on Information Theory, Vol 22, 1976, No 6, pp. 644-654.

[10] ElGamal, Taher. A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE transactions on information theory, Vol 31, 1985, No 4, pp. 469-472.

[11] Rabin, Michael O. Digitalized signatures and public-key functions as intractable as factorization, Massachusetts Inst of Tech Cambridge Lab for Computer Science, 1979.

[12] Nyberg K, Rueppel RA. Message recovery for signature schemes based on the discrete logarithm problem, InWorkshop on the Theory and Application of of Cryptographic Techniques Springer, Berlin, Heidelberg, 1994, pp. 182-193.

[13] Schnorr, Claus-Peter. Efficient signature generation by smart cards, Journal of cryptology Vol 4, 1991, No 3, pp. 161-174.

[14] Lauter, Kristin. The advantages of elliptic curve cryptography for wireless security. IEEE Wireless communications, vol 11, 2004, No 1, pp. 62-67.

[15] Hughes, Richard J., Douglas M. Alde, P. Dyer, Gabriel G. Luther, George L. Morgan, M. Schauer. Quantum cryptography, Contemporary Physics, Vol 36, 1995, No 3, pp. 149-163.

[16] Schneier, Bruce. Description of a new variable-length key, 64-bit block cipher (Blowfish), In International Workshop on Fast Software Encryption, Springer, Berlin, Heidelberg, 1993, pp. 191-204.

[17] Thakur, Jawahar, Nagesh Kumar. DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis, International journal of emerging technology and advanced engineering, Vol 1, 2011, No. 2, pp. 6-12.

[18] Daemen J, Rijmen V. The design of Rijndael: AES-the advanced encryption standard, Springer Science & Business Media, 2013.

[19] Leong, M.P., Cheung, O.Y., Tsoi, K.H. Leong, P.H.W. A bit-serial implementation of the international data encryption algorithm IDEA, In Proceedings 2000 IEEE Symposium on Field-Programmable Custom Computing Machines, IEEE, 2000, pp. 122-131.

[20] Charbathia S, Sharma S. A Comparative Study of Rivest Cipher Algorithms, International Journal of Information & Computation Technology, 2014, pp. 0974-2239.

[21] Ronald L.Rivest. The RC5 Encryption Algorithm, Proceedings of the 1994 Leuven Workshop on Fast Software Encryption, Springer Berlin Publishers, Vol 1008,1995, pp. 86-96.

[22] Rivest RL, Robshaw MJ, Sidney R, Yin YL. The RC6 TM block cipher, Advanced Encryption Standard (AES) Conference, 1998, pp. 16.

[23] Dobbertin H. Cryptanalysis of MD4, Workshop on Fast Software Encryption Springer, Berlin, Heidelberg, 1996, pp. 53-69.

[24] Rivest, Ronald. The MD5 message-digest algorithm, 1992.

[25] Gupta P, Kumar S. A comparative analysis of SHA and MD5 algorithm, Architecture, Vol 1, 2014, pp. 5.

[26] Dobbertin, Hans, Antoon Bosselaers, Bart Preneel. RIPEMD-160: A strengthened version of RIPEMD. International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 1996, pp. 71-82.

[27] Aumasson JP, Henzen L, Meier W, Phan RC. Sha-3 proposal blake. Submission to NIST: 92, 2008.

[28] Abhishek roy and Sunil karforma. A survey on digital signatures and its applications, Journal of Computer and Information Technology, Vol.3, 2012, No. 1&2, pp.45-69.

[29] Stallings W. Cryptography and Network Security, 4/E, Pearson Education India, 2006.