ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 8, February 2015

The State of Cryptography- A National Interest Perspective

JAVED MOHAMMED
Department of Computer Science, New York Institute of Technology Old Westbury, NY

***Abstract*--For every opportunity presented by the information age, there is an opening to invade the privacy and threaten the security of the nation, U.S. businesses, and citizens in their private lives. The more information that is transmitted in computer-readable form, the more vulnerable we become to automated spying. It's been estimated that some 10 billion words of computer-readable data can be searched for as little as $1. Rival companies can glean proprietary secrets, anti-U.S. terrorists can research targets, network hackers can do anything from charging purchases on someone else's credit card to accessing military installations. With patience and persistence, numerous pieces of data can be assembled into a revealing mosaic. Cryptography's Role in Securing the Information Society addresses the urgent need for a strong national policy on cryptography that promotes and encourages the widespread use of this powerful tool for protecting of the information interests of individuals, businesses, and the nation as a whole, while respecting legitimate national needs of law enforcement and intelligence for national security and foreign policy purposes.**

Cryptography if used with the latest measures will help the Department of Homeland and other federal and state agencies along with banks as well as major industries from losing millions of dollars as well as protect the public in safeguarding from future terrorist attacks. Cryptography is presently revolutionizing itself to help and safeguard our national interests and keep our economy strong with increase in job growth in fields related to cryptanalysis and cryptosystems.

This paper provides the cryptography goals, privacy, security, the cryptographic building blocks, modes of encryption/ decryption, secret key cryptography algorithms in use today, authentication, and information security concepts and illustrates in detail the challenges we face today. In order to obtain cyber security, we must secure data using cryptography and different keys. Also this research article illustrates a need for fundamental research in cryptography that ensures to create, deploy, and apply advanced cyber infrastructure program in ways that radically empower all scientific and engineering research and allied education.

***Index Terms*--** **cryptography, cyber infrastructure anti-U.S. terrorists, strong national policy, law enforcement and intelligence, national security, authentication, information security.**

I. INTRODUCTION

As information technology products and services begin to account for larger shares of international trade, and as companies engaging in foreign direct investment begin to focus more on high-technology areas with attendant risks to intellectual property, the importance of information security will continue to grow. A key component of any robust information security system is cryptography. Cryptography allows for the protection of sensitive information, either in storage or in communication, and is a necessary feature of any secure e-commerce or electronic communication system (including secure email and voice communication).. The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so. Cryptography has traditionally been a national-security issue, and several countries, especially U.S., have placed export controls on cryptography technology. Export controls intend to restrict international availability of this technology and cryptography products. U.S. export controls on have substantially slowed the proliferation of strong encryption to foreign adversaries over the years. Some countries like France or Russia have also import controls on cryptography. This is because the local government wants to be have full control over cryptography technology

In this age of universal electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed no time at which security does not matter. Two trends have come together to make the topic of this research of vital interest. First, the explosive growth in computer systems and their interconnections via networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This, in turn, has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks. Second, the disciplines of cryptography and network security have matured, leading to the development of practical, readily available applications to enforce network security

Cryptography is usually referred to as “the study of secret”. Encryption is the process of converting normal text to unreadable form. Decryption is the process of converting encrypted text to normal text in the readable form

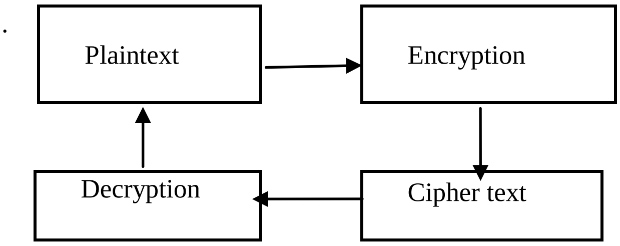

Fig 1: Conventional Encryption Model

Steps involved in the conventional encryption model:

- A sender wants to send a Hello message to a recipient.
- The original message, also called plaintext, is converted to random bits known as ciphertext by using a key and an

algorithm. The algorithm being used can produce a different output each time it is used, based on the value of the key.

- The cipher text is transmitted over the transmission medium.
- At the recipient end, the cipher text is converted back to the original text using the same algorithm and key that was used to encrypt the message.

Figure 1 below shows the conventional cryptographic process. As defined in RFC 2828, cryptographic system is “a set of cryptographic algorithms together with the key management processes that support use of the algorithms in some application context” [1] The definition gives the whole mechanism that provides the necessary level of security comprised of network protocols and data encryption algorithm

II. COMPUTER SECURITY

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications)

A. Cryptography Goals

Three key goals that are at the heart of computer security:

- ***Confidentiality:*** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information. This term covers two related concepts:
  - ***Data confidentiality***: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
  - ***Privacy***: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
- ***Integrity:*** Guarding against improper information modification or destruction, including ensuring information no repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information. This term covers two related concepts: Data integrity: Assures that information and programs are changed only in a specified and authorized manner. System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
- ***Availability***: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system Assures that systems work promptly and service is not denied to authorized users.

Additional goals

- Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
- *Accountability*: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes

B. Security Mechanisms

B.1 OSI Security Service

Mechanisms that are specific to any particular OSI security service or protocol layer:

- Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

- *Access Control*: A variety of mechanisms that enforce access rights to resources.
- *Data Integrity*: A variety of mechanisms used to assure the integrity of a data unit or stream of data units.
- Authentication Exchange: A mechanism intended to ensure the identity of an entity by means of information exchange.
- *Traffic Padding*: The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts. Routing Control Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
- *Notarization*: The use of a trusted third party to assure certain properties of a data exchange.

B.2Pervasive Security Mechanisms

Mechanisms that are not specific to any particular OSI security service or protocol layer.

- Trusted Functionality That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
- Security Label The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
- Event Detection of security-relevant events.
- Security Audit Trail Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
- Security Recovery Deals with requests from

mechanisms, such as event handling and management functions, and takes recovery actions.

B.3 Other Types of Security Mechanisms

Another type of unwanted access is the placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs, such as editors and compilers. Programs can present two kinds of threats:

- Information access threats: Intercept or modify data on behalf of users who should not have access to that data.
- Service threats: Exploit service flaws in computers to inhibit use by legitimate users. Viruses and worms are two examples of software attacks. Such attacks can be introduced into a system by means of a disk that contains the unwanted logic concealed in otherwise useful software. They can also be inserted into a system across a network; this latter mechanism is of more concern in network security.

The security mechanisms needed to cope with unwanted access fall into two broad categories:

- ➢ The first category might be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks. Once either an unwanted user or unwanted software gains access,
- ➢ The second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

Recovery:

- ➢ Selective-Field Connection Integrity: Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
- Connectionless Integrity: Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.
- Selective-Field Connectionless Integrity: Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

III. THE CRYPTOGRAPYHIC BUILDING BLOCKS

This paper describes, at a high level, the cryptographic underpinnings of the technology and why it provides such valuable elements with which to build a security infrastructure. Cryptography is fundamentally based on the use of keys that are used to encrypt and decrypt data [2] . There are two types of cryptography: 1) secret key or symmetric and 2) public key or asymmetric.

A. Symmetric Encryption

It is also called as single key cryptography. It uses a single key. In this encryption process the receiver and the sender has to agree upon a single secret (shared) key. Given a message (called plaintext) and the key, encryption produces unintelligible data, which is about the same length as the plaintext was. Decryption is the reverse of encryption, and uses the same key as encryption.

Secret key cryptography is characterized by the fact that the same key used to encrypt the data is used to decrypt the data. Clearly, this key must be kept secret among the communicating parties; otherwise the communication can be intercepted and decrypted by others. Until the mid 1970's, symmetric cryptography was the only form of cryptography available, so the same secret had to be known by all individuals participating in any application that provided a security service [3]. Although this form of cryptography was computationally efficient, it suffered from the fact that it could not support certain security services, and it presented a difficult key management problem since the secret keys had to be distributed securely to the communicating parties.

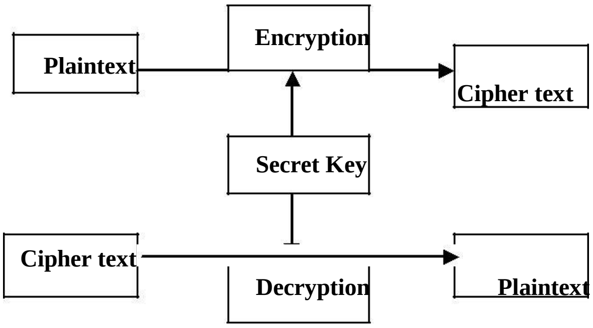

Fig 2: Symmetric Key Cryptography Process

However, this all changed when Whitfield Diffie and Martin Hellman introduced the notion of public key cryptography with the publication of their "New Directions in Cryptography" paper [DH] in 1976. This represented a significant breakthrough in cryptography because it enabled services that could not previously have been entertained as well as making traditional security services more expedient [4].

B. Asymmetric Encryption

It is also called as public key cryptography. It uses two keys: public key, which is known to the public, used for encryption and private key, which is known only to the user of that key, used for decryption. The public and the private keys are related to each other by any mathematical means. In other words, data encrypted by one public key can be encrypted only by its corresponding private key. Encryption and decryption procedure as shown below in figure 3.

Public key cryptography is based on the use of key pairs. When using a key pair, only one of the keys, referred to as the private key, must be kept secret and (usually) under the control of the owner. The other key, referred to as the public key, can be disseminated freely for use by any person who wishes to participate in security services with the person holding the private key. This is possible because the keys in the pair are mathematically related but it remains computationally infeasible to derive the private key from knowledge of the public key.

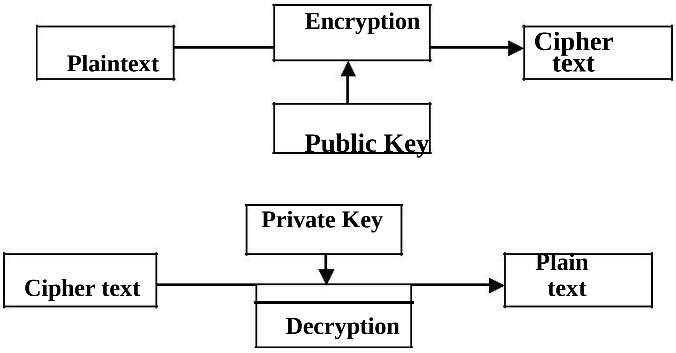

Fig 3: Public Key Cryptography Process

In theory, any individual can send the holder of a private key a message encrypted using the corresponding public key and ONLY the holder of the private key can read the secure message (i.e. can decrypt it). Similarly, the holder of the private key can establish the integrity and origin of the data he sends to another party by digitally signing the data using his private key. Anyone who receives that data can use the associated public key to validate that it came from the holder of the private key and verify the integrity of the data has been maintained [5].

This entire concept was revolutionary. One of its initial uses was to facilitate the delivery of keys to be used in symmetric cryptographic functions. Prior to this, the delivery of secret keys was arduous to set up and could not even be accomplished if the persons involved did not know each other. It also reduces the number of keys that must be used within a system. To keep communications secure using symmetric cryptography, each person in the system must have a different key for each person with whom he communicates; in the system of n users, there are on the order of n^2 keys. Under a public key scheme, there only needs to be one key pair per person in the system, or n key pairs in the system. This is a valuable advantage.

One significant factor that has been hand-waved until this point in the discussion is trust. Since transactions can be no more secure than the system in which they occur, the most important element becomes establishing a way for correspondents to locate each other and have confidence that the public key they use truly belongs to the person (or machine) with whom/which they wish to communicate. A Public Key Infrastructure is designed to provide this trust. Using a data element called a digital certificate or public key certificate, which binds a public key to identifying information about its owner, the infrastructure is designed to create the binding, and manage it for the benefit of all within the community of use [6]. Figure 4 illustrates the Version 3 public key certificate as defined in X.509.

Version	Serial	Signature	Issuer	Validity	Subject	Subject Public	Issuer	Subject	Optional	Digital Signature
	Number	(Info)				Key Info	Unique ID	Unique ID	Extensions	

Possible Extensions

Authority Key	Subject Key
Identifier	Identifier

Fig 4: Version 3 Public Key Certificate.

Data Fields and Extensions are defined in the X.509 standard. [Digitally Signed by Issuing CA]

C. Modes of Encryption/Decryption

ECB (Electronic Code Book)

In this mode data is divided into 64-bit blocks and each block is encrypted one at a time. Separate encryptions with different blocks are totally independent of each other. This means that if data is transmitted over a network or phone line, transmission errors will only affect the block containing the error. It also means, however, that the blocks can be rearranged, thus scrambling a file beyond recognition, and this action would go undetected. ECB is the weakest of the various modes because no additional security measures are implemented. However, ECB is the fastest and easiest to implement, making it the most common mode of DES seen in commercial applications. This is the mode of operation used by Private Encryptor.

CBC (Cipher Block Chaining):

In this mode of operation, each block of ECB encrypted ciphertext is XORed with the next plaintext block to be encrypted, thus making all the blocks dependent on all the previous blocks. This means that in order to find the plaintext of a particular block, you need to know the ciphertext, the key, and the ciphertext for the previous block. The first block to be encrypted has no previous ciphertext, so the plaintext is XORed with a 64-bit number called the Initialization Vector, or IV for short. So if data is transmitted over a network or phone line and there is a transmission error (adding or deleting bits), the error will be carried forward to all subsequent blocks since each block is dependent upon the last. If the bits are just modified in transit (as is the more common case) the error will only affect all of the bits in the changed block, and the corresponding bits in the following block. The error doesn't propagate any further. This mode of operation is more secure than ECB because the extra XOR step adds one more layer to the encryption process.

CFB (Cipher Feedback):

In this mode, blocks of plaintext those are less than 64 bits long can be encrypted. Normally, special processing has to be used to handle files whose size is not a perfect multiple of 8 bytes, but this mode removes that necessity (Private Encryptor handles this case by adding several dummy bytes to the end of a file before encrypting it). The plaintext itself is merely XORed with an output block from it, in the following manner A 64-bit block called the Shift Register is used as the input plaintext. This is initially set to some arbitrary value, and encrypted with the algorithm. The ciphertext is then passed through an extra component called the M-box, which simply selects the left-most M bits of the ciphertext, where M is the number of bits in the block we wish to encrypt. This value is XORed with the real plaintext, and the output of that is the final ciphertext. Finally, the ciphertext is fed back into the Shift Register, and used as the plaintext seed for the next block to be encrypted. As with CBC mode, an error in one block affects all subsequent blocks during data transmission. This mode of operation is similar to CBC and is very secure, but it is slower than ECB due to the added complexity.

OFB (Output Feedback): This is similar to CFB mode, except that the ciphertext output is fed back into the Shift Register, rather than the actual final ciphertext. The Shift Register is set to an arbitrary initial value, and passed through the algorithm. The output is passed through the M-box and then fed back into the Shift Register to prepare for the next block. This value is then XORed with the real plaintext (which may be less than 64 bits in length, like CFB mode), and the result is the final ciphertext. Note that unlike CFB and CBC, a transmission error in one block will not affect subsequent blocks because once the recipient has the initial Shift Register value; it will continue to generate new Shift Register plaintext inputs without any further data input. However, this mode of operation is less secure than CFB mode because only the real ciphertext and DES ciphertext output is needed to find the plaintext of the most recent block. Knowledge of the key is not required.

D. Secret Key Cryptography Algorithms in Use Today

Data Encryption Standard (DES):

The most common SKC scheme used today, DES was designed by IBM in the 1970s and adopted by the National Bureau of Standards (NBS) [now the National Institute for Standards and Technology (NIST)] in 1977 for commercial and unclassified government applications. DES is a block-cipher employing a 56-bit key that operates on 64-bit blocks. DES has a complex set of rules and transformations that were designed specifically to yield fast hardware implementations and slow software implementations, although this latter point is becoming less significant today since the speed of computer processors is several orders of magnitude faster today than twenty years ago. IBM also proposed a 112-bit key for DES, which was rejected at the time by the government; the use of 112-bit keys was considered in the 1990s, however, conversion was never seriously considered. Two important variants that strengthen DES are:

- Triple-DES (3DES): A variant of DES that employs up to three 56-bit keys and makes three encryption/decryption passes over the block; 3DES is also described in FIPS 46-3 and is the recommended replacement to DES.
- DESX: A variant devised by Ron Rivest. By combining 64 additional key bits to the plaintext prior to encryption, effectively increases the key length to 120 bits.
- Advanced Encryption Standard (AES): In 1997, NIST initiated a very public, 4-1/2 year process to develop a new secure cryptosystem for U.S. government applications. The result, the Advanced Encryption Standard, became the official successor to DES in December 2001. AES uses an SKC scheme called Rijndael, a block cipher designed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The algorithm can use a variable block length and key length; the latest specification allowed any combination of keys lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits. NIST initially selected Rijndael in October 2000 and formal adoption as the AES standard came in December 2001. FIPS PUB 197 describes a 128-bit block cipher employing a 128-, 192-, or 256-bit key.
- CAST-128/256: CAST-128, described in Request for Comments (RFC) 2144, is a DES-like substitution-permutation crypto algorithm, employing a 128-bit key operating on a 64-bit block.CAST-256 (RFC 2612) is an extension of CAST-128, using a 128-bit block size and a variable length (128, 160, 192, 224, or 256 bit) key. CAST is named for its developers, Carlisle Adams and Stafford Tavares and is available internationally. CAST-256 was one of the Round 1 algorithms in the AES process.
- International Data Encryption Algorithm (IDEA): Secret-key cryptosystem written by Xuejia Lai and James Massey, in 1992 and patented by

Ascom; a 64-bit SKC block cipher using a 128-bit key. Also available internationally.

- Rivest Ciphers (aka Ron's Code): Named for Ron Rivest, a series of SKC algorithms.

- RC1: Designed on paper but never implemented.

- RC2: A 64-bit block cipher using variable-sized keys designed to replace DES. It's code has not been made public although many companies have licensed RC2 for use in their products. Described in RFC 2268.

- RC3: Found to be breakable during development.

- RC4: A stream cipher using variable-sized keys; it is widely used in commercial cryptography products. An update to RC4, called Spritz, was designed by Rivest and Jacob Schuldt.

- RC5: A block-cipher supporting a variety of block sizes (32, 64, or 128 bits), key sizes, and number of encryption passes over the data. Described in RFC 2040.

- RC6: A 128-bit block cipher based upon, and an improvement over, RC5; RC6 was one of the AES Round 2 algorithms.

- Blowfish: A symmetric 64-bit block cipher invented by Bruce Schneier; optimized for 32-bit processors with large data caches, it is significantly faster than DES on a Pentium/PowerPC-class machine. Key lengths can vary from 32 to 448 bits in length. Blowfish, available freely and intended as a substitute for DES or IDEA, is in use in a large number of products.

- Two fish: A 128-bit block cipher using 128-, 192-, or 256-bit keys. Designed to be highly secure and highly flexible, well-suited for large microprocessors, 8-bit smart card microprocessors, and dedicated hardware. Designed by a team led by Bruce Schneier and was one of the Round 2 algorithms in the AES process.

Camellia: A secret-key, block-cipher crypto algorithm developed jointly by Nippon Telegraph and Telephone (NTT) Corp. and Mitsubishi Electric Corporation (MEC) in 2000. Camellia has some characteristics in common with AES: a 128-bit block size, support for 128-, 192-, and 256-bit key lengths, and suitability for both software and hardware implementations on common 32-bit processors as well as 8-bit processors (e.g., smart cards, cryptographic hardware, and embedded systems). Also described in RFC 3713. Camellia's application in IPsec is described in RFC 4312 and application in Open PGP in RFC 5581.

- MISTY1: Developed at Mitsubishi Electric Corp., a block cipher using a 128-bit key and 64-bit blocks, and a variable number of rounds. Designed for hardware and software implementations, and is resistant to differential and linear cryptanalysis. Described in RFC 2994.

- Secure and Fast Encryption Routine (SAFER): Secret-key crypto scheme designed for implementation in software. Versions have been defined for 40-, 64-, and 128-bit keys.
- KASUMI: A block cipher using a 128-bit key that is part of the Third-Generation Partnership Project (3gpp), formerly known as the Universal Mobile Telecommunications System (UMTS). KASUMI is the intended confidentiality and integrity algorithm for both message content and signaling data for emerging mobile communications systems.
- SEED: A block cipher using 128-bit blocks and 128-bit keys. Developed by the Korea Information Security Agency (KISA) and adopted as a national standard encryption algorithm in South Korea. Also described in RFC 4269.

- ARIA: A 128-bit block cipher employing 128-, 192-, and 256-bit keys. Developed by large group of researchers from academic institutions, research institutes, and federal agencies in South Korea in 2003, and subsequently named a national standard. Described in RFC 5794.

- CLEFIA: Described in RFC 6114, CLEFIA is a 128-bit block cipher employing key lengths of 128, 192, and 256 bits (which is compatible with AES). The CLEFIA algorithm was first published in 2007 by Sony Corporation. CLEFIA is one of the new-generation lightweight block cipher algorithms designed after AES, offering high performance in software and hardware as well as a lightweight implementation in hardware.

- SMS4: SMS4 is a 128-bit block cipher using 128-bit keys and 32 rounds to process a block. Declassified in 2006, SMS4 is used in the Chinese National Standard for Wireless Local Area Network (LAN) Authentication and Privacy Infrastructure (WAPI). SMS4 had been a proposed cipher for the Institute of Electrical and Electronics Engineers (IEEE) 802.11i standard on security mechanisms for wireless LANs, but has yet to be accepted by the IEEE or International Organization for Standardization (ISO). SMS4 is described in SMS4 Encryption Algorithm for Wireless Networks (translated and typeset by Whitfield Diffie and George Ledin, 2008) or in the original Chinese.

- Skipjack: SKC scheme proposed for Capstone. Although the details of the algorithm were never made public, Skipjack was a block cipher using an 80-bit key and 32 iteration cycles per 64-bit block.

- GSM (Global System for Mobile Communications, originally Groupe Special Mobile) encryption: GSM mobile phone systems use several stream ciphers for over-the-air communication privacy. A5/1 was developed in 1987 for use in Europe and the

U.S. A5/2, developed in 1989, is a weaker algorithm and intended for use outside of Europe and the U.S. Significant flaws were found in both ciphers after the "secret" specifications were leaked in 1994, however, and A5/2 has been withdrawn from use. The newest version, A5/3, employs the KASUMI block cipher. **NOTE:** Unfortunately, although A5/1 has been repeatedly "broken", this encryption scheme remains in widespread use, even in 3G and 4G mobile phone networks. Use of this scheme is reportedly one of the reasons that the National Security Agency (NSA) can easily decode voice and data calls over mobile phone networks.

- GPRS (General Packet Radio Service) encryption: GSM mobile phone systems use GPRS for data applications, and GPRS uses a number of encryption methods, offering different levels of data protection. GEA/0 offers no encryption at all. GEA/1 and GEA/2 are proprietary stream ciphers, employing a 64-bit key and a 96-bit or 128-bit state, respectively. GEA/1 and GEA/2 are most widely used by network service providers today although both have been reportedly broken. GEA/3 is a 128-bit block cipher employing a 64-bit key that is used by some carriers; GEA/4 is a 128-bit clock cipher with a 128-bit key, but is not yet deployed.

- Cipher-2: Described in RFC 7008, KCipher-2 is a stream cipher with a 128-bit key and a 128-bit initialization vector. Using simple arithmetic operations, the algorithms offers fast encryption and decryption by use of efficient implementations. KCipher-2 has been used for industrial applications, especially for mobile health monitoring and diagnostic services in Japan.

IV. AUTHENTICATION

The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be. Second, the service must assure that the connection is not interfered with in such a way that a third party can be one of the two legitimate parties for the purposes of unauthorized transmission or reception. Two specific authentication services are defined in X.800:

Peer entity authentication: Provides for the corroboration of the identity of a peer entity in an association. Two entities are considered peers if they implement to same protocol in different systems; e.g., two TCP modules in two communicating systems. Peer entity authentication is provided for use at the establishment of, or at times during the data transfer phase of, a connection [7]. It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.

- Data origin authentication: Provides for the corroboration of the source of a data unit. It does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail, where there are no prior interactions between the communicating entities

A. *Message Authentication Functions*

Any message authentication or digital signature mechanism has two levels of functionality. At the lower level, there must be some sort of function that produces an authenticator: a value to be used to authenticate a message. This lower-level function is then used as a primitive in a higher-level authentication protocol that enables a receiver to verify the authenticity of a message. This mechanism is concerned with the types of functions that may be used to produce an authenticator. These may be grouped into three classes.

- Hash function: A function that maps a message of any length into a fixed length hash value , which serves as the authenticator A hash function H accepts a variable-length block of data as input and produces a fixed-size hash value $h = H(M)$. A “good” hash function has the property that the results of applying the function to a large set of inputs will produce outputs that are evenly distributed and apparently random. In general terms, the principal object of a hash function is data integrity. A change to any bit or bits in results, with high probability, in a change to the hash code. The kind of hash function needed for security applications is referred to as a cryptographic hash function.

- A cryptographic hash function is an algorithm for which it is computationally infeasible (because no attack is significantly more efficient than brute force) to find either (a) a data object that maps to a pre-specified hash result (the one-way property) or (b) two data objects that map to the same hash result (the collision-free property). Because of these characteristics, hash functions are often used to determine whether or not data has changed.

- Message encryption: The ciphertext of the entire message serves as its authenticator
- Message authentication code (MAC): A function of the message and a secret key that produces a fixed-length value that serves as the authenticator.

B. *Message Authentication*

Message authentication is a mechanism or service used to verify the integrity of a message. Message authentication assures that data received are exactly as sent (i.e., contain no modification, insertion, deletion, or replay). In many cases, there is a requirement that the authentication mechanism assures that purported identity of the sender is valid. When a hash function is used to provide message authentication, the hash function value is often referred to as a message digest [8]. More commonly, message authentication is achieved using a message authentication code (MAC), also known as a keyed hash function. Typically, MACs are used between two parties that share a secret key to authenticate information exchanged between those parties. A MAC function takes as input a secret key and a data block and produces a hash value, referred to as the MAC. This can then be transmitted with or stored with the protected message. If the integrity of the message needs to be checked, the MAC function can be applied to the message and the result compared with the stored MAC value. An attacker who alters the message will be unable to alter the MAC value without knowledge of the secret key [9]. Note that the verifying party also knows who the sending party is because no one else knows the secret key. A MAC function is similar to encryption. One difference is that the MAC algorithm need not be reversible, as it must be for decryption. In general, the MAC function is a many-to-one function. The domain of the function consists of messages of some arbitrary length, whereas the range consists of all possible MACs and all possible keys.

C. Applications

C.1 Hash Functions

Hash functions are commonly used to create a one-way password file. Thus, the actual password is not retrievable by a hacker who gains access to the password file. In simple terms, when a user enters a password, the hash of that password is compared to the stored hash value for verification. This approach to password protection is used by most operating systems. Hash functions can be used for intrusion detection and virus detection

C.2 Digital Signatures

Another important application, which is similar to the message authentication application, is the digital signature. The operation of the digital signature is similar to that of the MAC. In the case of the digital signature, the hash value of a message is encrypted with a user's private key. Anyone who knows the user's public key can verify the integrity of the message that is associated with the digital signature. In this case, an attacker who wishes to alter the message would need to know the user's private key.

V. PRIVACY

An issue with considerable overlap with computer security is that of privacy. On the one hand, the scale and interconnectedness of personal information collected and stored in information systems has increased dramatically, motivated by law enforcement, national security, and economic incentives [10]. The last mentioned has been perhaps the main driving force.

Privacy (or "secrecy") is the cornerstone of applied cryptography. A commonly desired form of security is making data readable only by certain intended recipients. Whether symmetric or public key cryptography is in use, a person (or machine) proves that they are an intended recipient by possessing the key that can be used to decrypt the message. In the case of simply achieving privacy, it really doesn't matter whether symmetric or public key encryption is used; public key encryption is very slow, so in practice, it's only used to encrypt a symmetric key that is used to encrypt the rest of the data [11].

Privacy is commonly desired when sensitive data is being transmitted. In the case of web browsing, this is one of the purposes of the Secure HTTP (HTTPS) protocol. When communicating with, for example, your bank's website, it is important that the information being transacted is private. It is highly undesirable for any other person, even a professional network administrator at your ISP, who happens to control a computer on the Internet through which the data between you and your bank passes, to be able to look at your account numbers and balances [12][13]. Similarly, if you store sensitive corporate information or highly personal documents on a laptop, you would want to make sure that these documents remain private if the laptop were ever lost or stolen. For this, you would encrypt the files (or better yet the entire hard drive) and either keep the decryption key outside of the laptop, or keep it protected with a strong passphrase. In the latter case, the passphrase itself is the key to a cryptographic algorithm will provide the unencrypted version of the decryption key for your files or hard drive, and the passphrase is ideally stored only in your head [14].

In a global information economy, it is likely that the most economically valuable electronic asset is aggregations of information on individuals . On the other hand, individuals have become increasingly aware of the extent to which government agencies, businesses, and even Internet users have access to their personal information and private details about their lives and activities. Concerns about the extent to which personal privacy has been and may be compromised have led to a variety of legal and technical approaches to reinforcing privacy rights

A. United States Privacy Initiatives

The first comprehensive privacy legislation adopted in the United States was the Privacy Act of 1974, which dealt with personal information collected and used by federal agencies [15]. The Act is intended to

- Permit individuals to determine what records pertaining to them are collected, maintained, used, or disseminated.
- Permit individuals to forbid records obtained for one purpose to be used for another purpose without consent.
- Permit individuals to obtain access to records pertaining to them and to correct and amend such records as appropriate.
- Ensure that agencies collect, maintain, and use personal information in a manner that ensures that the information is current, adequate, relevant, and not excessive for its intended use.
- Create a private right of action for individuals whose personal information is not used in accordance with the Act.

As with all privacy laws and regulations, there are exceptions and conditions attached to this Act, such as criminal investigations, national security concerns, and conflicts between competing individual rights of privacy. While the 1974 Privacy Act covers government records, a number of other U.S. laws have been enacted that cover other areas, including the following [16]:

- Banking and financial records: Personal banking information is protected in certain ways by a number of laws, including the recent Financial Services Modernization Act.
- Credit reports: The Fair Credit Reporting Act confers certain rights on individuals and obligations on credit reporting agencies.
- Medical and health insurance records: A variety of laws have been in place for decades dealing with medical records privacy. The Health Insurance Portability and Accountability Act (HIPPA) created significant new rights for patients to protect and access their own health information.
- Children's privacy: The Children's Online Privacy Protection Act places restrictions on online organizations in the collection of data from children under the age of 13.

Electronic communications: The Electronic Communications Privacy Act generally prohibits unauthorized and intentional interception of wire and electronic communications during the transmission phase and unauthorized accessing of electronically stored wire and electronic communications.

B. *Privacy and Data Surveillance*

The demands of homeland security and counterterrorism have imposed new threats to personal privacy. Law enforcement and intelligence agencies have become increasingly aggressive in using data surveillance techniques to fulfill their mission. In addition, private organization are exploiting a number of trends to increase their ability to build detailed profiles of individuals, including the spread of the Internet, the increase in electronic payment methods, near-universal use of cellular phone communications, ubiquitous computation, sensor webs, and so on [17]. Both policy and technical approaches are needed to protect privacy when both government and nongovernment organizations seek to learn as much as possible about individuals. In terms of technical approaches, the requirements for privacy protection for information systems can be addressed in the context of database security. That is, the approaches that are appropriate for privacy protection involve technical means that have been developed for database security.

A cryptographically protected device that is interposed between a database and the access interface, analogous to a firewall or intrusion prevention device implements privacy protection functions, including verifying the user's access permissions and credentials and creating an audit log. Some of the specific functions of the device are as follows:

Data transformation: This function encodes or encrypts portions of the data so as to preserve privacy but still allow data analysis functions needed for effective use. An example of such data analysis functions is the detection of terrorist activity patterns.

- Anonymization: This function removes specific identifying information from query results, such as last name and telephone number, but creates some sort of anonymized unique identifier so that analysts can detect connections between queries.
- Selective revelation: This is a method for minimizing exposure of individual information while enabling continuous analysis of potentially interconnected data. The function initially reveals information to the analyst only in sanitized form, that is, in terms of statistics and categories that do not reveal (directly or indirectly) anyone's private information. If the analyst sees reason for concern, he or she can follow up by seeking permission to get more precise information. This permission would be granted if the initial information provides sufficient cause to allow the revelation of more information, under appropriate legal and policy guidelines.
- Immutable audit: A tamper-resistant method that identifies where data go and who has seen the data. The audit function automatically and permanently records all data accesses, with strong protection against deletion, modification, and unauthorized use.
- Associative memory: This is a software module that can recognize patterns and make connections between pieces of data that the human user may have missed or didn't know existed. With this method, it can discover relationships quickly between data points found in massive amounts of data.

C. *Types of Computer Crime*

Computer crime, or cybercrime, is a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity. These categories are not exclusive, and many activities can be characterized as falling in one or more categories. The term cybercrime has a connotation of the use of networks specifically, whereas computer crime may or may not involve networks [18]. The U.S. Department of Justice [DOJ00] categorizes computer crime based on the role that the computer plays in the criminal activity, as follows:

- Computers as targets: This form of crime targets a computer system, to acquire information stored on that computer system, to control the target system without authorization or payment (theft of service), or to alter the integrity of data or interfere with the availability of the computer or server. This form of crime involves an attack on data integrity, system integrity, data confidentiality, privacy, or availability.
- Computers as storage devices: Computers can be used to further unlawful activity by using a computer or a computer device as a passive storage medium. For example, the computer can be used to store stolen

password lists credit card or calling card numbers, proprietary corporate information, pornographic image files, or “warez” (pirated commercial software).

- Computers as communications tools: Many of the crimes falling within this category are simply traditional crimes that are committed online. Examples include the illegal sale of prescription drugs, controlled substances, alcohol, and guns; fraud; gambling; and child pornography

As stated earlier, Whitfield Diffie and Martin Hellman first introduced the notion of public key cryptography in 1976 with the publication of“New Directions in Cryptography” [DH]. A great deal of progress has been made since then, including the development of public key cryptographic algorithms such as RSA [RSA], DSA [DSA], and the class of cryptographic algorithms based on Elliptic Curve Cryptography [ECC]. How-ever, it is only within the last 10 years or so that technology has become available to manage the public/private key pairs. This managed solution is referred to as Public Key Infrastructure (PKI), and it provides the foundation for offering scalable key and certificate life cycle management [19].

VI. THE CHALLENGES

Computer and network security is both fascinating and complex. Some of the reasons follow:

- Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, non repudiation, or integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning.
- In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.
- Because of the above statement, the procedures used to provide particular services are often counterintuitive. Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.
- Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such as TCP/IP (Transmission Control Protocol/Internet Protocol) should mechanisms be placed].
- Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There also may be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism. For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or network that introduces variable, unpredictable delays may render such time limits meaningless.
- Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.
- There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.
- Security requires regular, even constant, monitoring, and this is difficult in today’s short-term, overloaded environment.
- Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.
- Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

A. Law Enforcement Challenges

The deterrent effect of law enforcement on computer and network attacks correlates with the success rate of criminal arrest and prosecution. The nature of cybercrime is such that consistent success is extraordinarily difficult. For law enforcement agencies, cybercrime presents some unique difficulties. Proper investigation requires a fairly sophisticated grasp of the technology [20]. Although some agencies, particularly larger agencies, are catching up in this area, many jurisdictions lack investigators knowledgeable and experienced in dealing with this kind of crime. Lack of resources represents another handicap. Some cybercrime investigations require considerable computer processing power, communications capacity, and storage capacity, which may be beyond the budget of individual jurisdictions [21]. The global nature of cybercrime is an additional obstacle: Many crimes will involve perpetrators who are remote from the target system, in another jurisdiction or even another country. A lack of collaboration and cooperation with remote law enforcement agencies can greatly hinder an investigation. Initiatives such as the international Convention on Cybercrime are a promising sign.

VII. CONCLUSION

This paper has briefly described the goals of cryptography, the privacy and security measures and the challenge we face to counterattack from adversaries. It also explores how all of us are affected by information security issues: private companies and businesses; law enforcement and other agencies; people in their private lives. This article takes a realistic look at what cryptography can and cannot do and how its development has been shaped by the forces of supply and demand. The new set of cryptographic algorithms has become the preferred global standard for ensuring the security and integrity of information shared over non-trusted networks. These algorithms helps public and private sector organizations meet compliance. requirements, including Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Processing Standards (FIPS), and others.

REFERENCES

[1] Nagesh K, Jawahar Thakur, Arvind K (2011) " Performance Analysis of Symmetric Key Cryptography Algorithms: Des, Aes and Blowfish".

[2] Barry K Shelton, "Information to Security", http://www.infosectoday.com/Articles/ Intro_to_Cryptography/Introduction_Encryption_Algorithms. htm.

[3] Steve Lloyd, et al, PKI Basics - A Technical Perspective: "The Cryptographic Building Blocks".

[4] Whitfield Diffie and Martin E. Hellman, (1976) “New Directions in Cryptography".

[5] Arif Arman, (2014) “Digital Signature Certificate of dataedgeid of data edge Ltd", Aftabnagar, Dhaka 1212.

[6] D. Richard Kuhn Vincent C. Hu, et al, Introduction to Public Key Technology and the Federal PKI Infrastructure 2011.

[7] William Stallings, EDN Network, " Cryptography and Network Security: The basics—Part III", 2013.

[8] Elaine Barker, William Barker, et al, "Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930 July 2012".

[9] Donna F. Dodson W. Timothy Polk, et al, “Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, April 2006".

[10] James Waldo, Herbert S. Lin, et al, Thinking About Privacy: Chapter 1 of “Engaging Privacy and Information Technology in a Digital Age”, Journal of Privacy and Confidentiality (2010) 2, Number 1, pp. 19–50.

[11] Leemon C. Baird, "Network Security” Colorado Research Institute for Security and Privacy University of Denver, Denver, CO 80208. USA.

[12] Tom Szuba, "Safeguarding Your Technology", U.S. Department of Education. National Center for Education Statistics. Safeguarding Your Technology, NCES. Washington, DC. 1998.

[13] Rica Weller, Ross Clements, et al, IBM "Introduction to the New Mainframe: Security” March 2007.

[14] Navigating PCI DSS: Understanding the Intent of the Requirements, v2.0 October 2010 Copyright 2010 PCI Security Standards Council LLC.

[15] Paula Seli, Anita Ramasastry, et al., Consumer Privacy And Data Protection Protecting Personal Information Through Commercial Best Practices, August 27, 2001.

[16] Michael McFarland, SJ, "Information Privacy: A Case Study and Commentary" http://articles.latimes.com/2011/jul/08/local/la-me-celebrity-snooping-20110708.

[17] Georgios Tselentis, John Domingue, et al., "Towards the Future Internet” ISBN 978-1-60750-007-0 Library of Congress Control Number: 2009925664.

[18] H. Marshall Jarrett, et al., "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", September 2002.

[19] Diffie, W., & Landau, S. (1998). Privacy on the Line. Boston: MIT Press.

[20] Edward J. Tully, "Meeting Law Enforcements Responsibilities Solving the Serious Issues of Today", September, 2011.

[21] George Grispos, Tim Storer, et al., International Journal of Cloud Computing in Digital Forensics, Volume 4, Issue 2, Pages 28-48.

AUTHOR BIOGRAPHY

Javed Mohammed was born in Hyderabad, India, in1990. He received his Master’s Science in Computer Science from NewYork Institute of Technology About to pursue PhD in Geospatial Computing from Texas A&M Corpus Christi. Presently taking advanced courses in Computer Science from Massachusetts University of Technology (MIT) & Harvard University.

In 2014, he worked on various multi-disciplinary projects in Computer Science, Geospatial Intelligence projects. His current research interests include Nanotechnology, Cyber Security, Cryptography, Database Management, Cloud Computing and Big Data, Software Systems, Modeling and Simulation of Water Quality at Hydro racking operations, Mobile and Wireless Computing, and Programming Languages.

He is currently serving on the editorial board of “ International Journal of Computer Science, Engineering and Applications (IJCSEA); as a Technical program committee member of “4th International Conference on Advances in Computing, Communications and Informatics”; as a Program committee member of “Fifth International conference on Computer Science, Engineering and Applications”; as judge for peer-reviewed presentations at prestigious International Conferences; and was invited to White House AAPI <WhiteHouseAAPI@ed.gov> to attend the Asian American and Pacific Islander (AAPI) Heritage Month Opening Ceremony. Mr. Mohammed also organized a Presidential Initiative on “Second Annual National Day of Civic Hackathon”.

Mr. Mohammed is a member of Association for Computing Machinery (ACM) ;Ground Water Protection Council (GWPC); National Society of Professional Engineering; SAS Data Management; Association of Environment and Engineering Geologists (AEG); Information System Security Association (ISSA); American Society of Administrative Professionals (ASAP); Big Data Innovation Group; and Fracfocus.