An Analysis of Hybrid Cryptographic Approaches for Information Security

Neetha Francis
Research Scholar
Department of IT, Mangattuparambu Campus
Kannur, Kerala.

Thomas Monoth
Dept. of Computer Science
Mary Matha Arts & Science College
Mananthavady, Wayanad, Kerala

Abstract—Secure communication is vital to facilitate confidential exchange of information between any sender and receiver. The security of information passed over an open channel has become a fundamental issue and therefore confidentiality, authentication and data integrity are required. Information Security is the process of protecting information from unauthorized access. Cryptographic techniques are used for the purpose of making the exchange of information secure. Almost all cryptosystems are vulnerable to different types of cryptographic attacks. Hence there is a need to protect the system by using combinations of cryptographic algorithms. Hybridization of algorithms is a useful scheme that provides solutions to some major problems in the communication networks. A detailed analysis of various hybrid cryptosystems proposed by different researchers is done thereby listing the features of the algorithms used in hybrid cryptography.

Keywords—hybrid cryptosystem, symmetric key cryptography, public key cryptography, hash algorithm

I. INTRODUCTION

Research analysis of information security attracts many researchers, because of its importance in the growing field of electronic communications. Large amount of sensitive information such as health and legal records, financial transactions, credit ratings are frequently exchanged between computers through public communication facilities and these messages must be kept confidential and protected against manipulation. Cryptography deals with the transformation of plaintext into cipher text by encryption and transformation of cipher text back into plaintext by decryption. It ensures privacy, trust, access control in e-payments, e-voting, corporate security and in many other applications.

In majority of cryptographic applications in practical systems, symmetric and asymmetric algorithms and also hash functions are all used together. This is referred to as hybrid schemes. The reason for using both families of algorithms is that each has specific strengths and weaknesses. Symmetric ciphers are significantly faster, at least 1000 times faster than asymmetric ciphers, but require all parties to somehow share the key.

Cryptography is the science/art of securing messages [1]. It is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, authentication, and availability. It is the scrambling of the content of the data, such as text, image, audio, video and so forth to make the data unreadable or meaningless during transmission or storage. The schemes used for enciphering messages constitute the area of study known as cryptography. On the other hand, cryptanalysis is the science/art of breaking the cipher [2]. It is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

Cryptographic algorithms are broadly classified into three categories:

A. Secret Key Cryptography:
This type of cryptography technique uses a single key. The sender applies a key to encrypt a message while the receiver applies the same key to decrypt the message. Since only single key is used it is called as symmetric encryption or private key cryptography [3].

B. Public Key Cryptography:
This type of cryptographic technique involves two keys. One key is used for encryption and the other for decryption. Since a pair of keys is applied here, this technique is also known as asymmetric encryption. In this method, each party has a private key and a public key. The private is kept secret and is not revealed while the public key is shared with all those whom we want to communicate with.

C. Hash Functions:
A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, or simply hashes. A cryptographic hash function allows one to easily verify that some input data maps to a given hash value. But if the input data is unknown, it is difficult to reconstruct it by knowing the stored hash value. This is used for assuring integrity of transmitted data.

II. HYBRID CRYPTOGRAPHY
Hybrid encryption is a mode of encryption that merges two or more encryption systems. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security. Hybrid encryption is considered a highly secure type of encryption as long as the public and private keys are fully secure. A hybrid encryption scheme is one that blends the convenience of an asymmetric encryption scheme with the effectiveness of a symmetric encryption scheme. The combination of encryption methods has various advantages. Users then have the ability to communicate through hybrid encryption. Asymmetric encryption can slow down the encryption process, but with the simultaneous use of symmetric encryption, both forms of encryption are enhanced. The result is the added security of the transmittal process along with overall improved system performance.

The main aim of this paper is to study and analyze the advantages of Hybrid Cryptography. It is important to secure the information exchange over the internet and for local storage of confidential data. Cryptography provides authenticated communication over untrusted channels, as long as the secret keys are not exposed. However, attacks by hackers and insiders often expose secret keys. Such break-in attacks often control the systems only for a limited time, and therefore security may be regained, provided new keys can be selected and installed with precision. This proactive recovery operation must be invoked periodically, since the exposure may remain undetected. The arrival of the information technology age was so rapid that we have not yet managed to cope with all the changes or with many of the consequences. More and more people are concerned about the issue of privacy in an age in which virtually everything we do is recorded somewhere in a computer system and communicated through some electronic means. Fig. 1 depicts the basic model of a hybrid cryptosystem.

### III. SOME IMPORTANT ALGORITHMS USED IN HYBRID CRYPTOGRAPHY

#### A. DES (Data Encryption Standard)

The Data Encryption Standard is one of the first commercially developed ciphers. DES is a block cipher that encrypts 64-bit data blocks and encryption of the data is performed using a 56-bit secret key [4]. DES consists of sixteen rounds and two permutation layers. DES uses a shared key both to encrypt and decrypt the message. The decryption process is the reverse of encryption process. DES possesses strong Avalanche effect and is flexible as it works in CBC, ECB, CFB and OFB modes. DES is vulnerable to Brute Force attack and relatively slow.

#### B. AES (Advanced Encryption Standard)

The algorithm was invented by Joan Daemen and Vincent Rijmen. AES can process 128 bit data block and uses key lengths of 128, 192, or 256 bits. For the key length of 128,192 and 256 bits, AES may be referred to as AES-128, AES-192 and AES-256 respectively. Unlike DES, AES has no fiestel structure. Number of rounds in AES depends on key length i.e. for a key length of 128, number of rounds is 10 and similarly for 192 and 256 bit keys, it is 12 and 14 respectively. AES provides resistance against all known attacks, simple in design and good speed of computation.

#### C. RSA (Rivest, Shamir and Adleman)

A public key encryption algorithm developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977. It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key encryption. It is still widely used in electronic commerce protocols, and is believed that its security depends on the difficulty of decomposition of large numbers. RSA is secure because it is able to resist concerted attack.
D. Diffie-Hellman Key Exchange Algorithm

Whitfield Diffie and Martin Hellman discovered Diffie-Hellman (DH) algorithm in 1976 was the first public key algorithm ever invented. Diffie–Hellman establishes a shared secret key that can be used for secret communications by exchanging data over a public network. Diffie–Hellman algorithm does not need any known key before communication begins and Discrete Logarithm Problem makes it extremely difficult to crack. Diffie–Hellman algorithm is vulnerable to man-in-the-middle attack.

E. Elgamal Algorithm

Elgamal algorithm was invented by Taher El-Gamal which is based on Discrete Logarithm Problem and Diffie-Hellman key exchange. Elgamal can be used for encryption as well as digital signature. Each time when the same plaintext is encrypted, it gives a different ciphertext. Elgamal has the disadvantage of having ciphertext twice the size of the plaintext.

F. DSA (Data Signature Algorithm)

Data Signature Algorithm was invented by David Kravitz. Digital Signature Standard (DSS) used DSA proposed by National Institute of Standards and Technology (NIST) in 1991. Security of DSA is based on the difficulty to solve discrete logarithms. DSA has been accepted widely. DSA is more efficient and faster than RSA.

G. ECC (Elliptic Curve Cryptography)

The use of elliptic curves in public key cryptography was independently proposed by Koblitz and Miller in 1985 and since then, an enormous amount of work has been done on elliptic curve cryptography. The basic EC operations are point addition and point doubling. Simple multiplication could not be found in the case of elliptic curves. A single point suppose A(x, y) on the elliptic curve could yield a resultant point B(x’, y’) by following a series of point addition and point doubling instead of directly multiplying the point A with a scalar, hence A=zB, where z is a scalar multiple.

In practice, the symmetric key algorithms and public key cryptography algorithms are generally combined together. Combining the features of two algorithms for the sake of better efficiency and performance is known as Hybrid cryptography. Hybridization of algorithms is a useful scheme that provides solutions to some major problems in the communication networks. Deploying the positive points of an algorithm into another less efficient algorithms will result in new hybrid cryptographic algorithm. An analysis and study on different algorithms used in hybrid cryptography is performed by reviewing research articles of various researchers and given in Table 1.

IV. ANALYSIS OF DIFFERENT ALGORITHMS AND THEIR ADVANTAGES

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Author</th>
<th>Year of publication</th>
<th>Cryptography algorithms used in Hybrid Cryptosystem</th>
<th>Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tayal N et al.[4]</td>
<td>2017</td>
<td>Huffman coding, hierarchical encryption technique</td>
<td>Good security, high robustness, low computation time, high data embedding capacity</td>
</tr>
<tr>
<td>2</td>
<td>N Mathur et al.[5]</td>
<td>2016</td>
<td>AES, ECC</td>
<td>Secure key exchange, enhanced cipher text security, prevents timing side channel attacks</td>
</tr>
<tr>
<td>3</td>
<td>MIS Reddy et al.[6]</td>
<td>2016</td>
<td>AES, LSB</td>
<td>Increased security as text embedded in the wavelet transformed image</td>
</tr>
<tr>
<td>4</td>
<td>L D Singh et al.[7]</td>
<td>2015</td>
<td>Modified ECC with ASCII values</td>
<td>Equal security with less key size, saves bandwidth, suitable for devices with limitations in power, storage and processing</td>
</tr>
<tr>
<td>5</td>
<td>R Rizk et al.[8]</td>
<td>2015</td>
<td>ECC, AES, XOR Dual RSA, MD5</td>
<td>Better security, reduced processing overhead, lower energy consumption</td>
</tr>
<tr>
<td>6</td>
<td>K Goodarzi c. al.[9]</td>
<td>2014</td>
<td>Caesar Cipher, DES</td>
<td>More secured, maintaining the confidentiality of data</td>
</tr>
<tr>
<td>7</td>
<td>S K Sinha et al.[10]</td>
<td>2013</td>
<td>Enhanced symmetric key algorithm</td>
<td>More efficient for large data, better speed, less overhead</td>
</tr>
<tr>
<td>8</td>
<td>Bansod et al.[11]</td>
<td>2012</td>
<td>DES, RSA</td>
<td>Two levels of security i.e. hybrid cryptography and steganography are combined together. BPCS approach is used to decide embedding byte positions.</td>
</tr>
<tr>
<td>---</td>
<td>-----------------</td>
<td>------</td>
<td>---------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>9</td>
<td>Dhakar et al.[12]</td>
<td>2012</td>
<td>Modified RSA</td>
<td>More secure against mathematical and brute force attacks. It works on dual modulus and used for both encryption and signing.</td>
</tr>
<tr>
<td>10</td>
<td>Gutub and Khan[13]</td>
<td>2012</td>
<td>DES(56 bit key)</td>
<td>Key encryption with RSA, data encryption with DES &amp; AES. Faster in execution and provides maximum security</td>
</tr>
<tr>
<td>11</td>
<td>S Gupta et al.[14]</td>
<td>2012</td>
<td>RSA</td>
<td>Provides communication security, avoids attacks, confidential messages can be transferred.</td>
</tr>
<tr>
<td>12</td>
<td>Zhang and Jin[15]</td>
<td>2012</td>
<td>AES(128 bit key)</td>
<td>Triple DES for confidentiality, RSA for key management and SHA-1 for data integrity.</td>
</tr>
<tr>
<td>13</td>
<td>Wang and Zhang[16]</td>
<td>2011</td>
<td>RSA cryptography</td>
<td>Transformation of personal information from plaintext to cipher text can be done and client’s privacy is preserved.</td>
</tr>
</tbody>
</table>

V. CONCLUSION

Privacy is one of the key issues addressed by information Security. Through cryptographic encryption methods, one can prevent a third party from understanding transmitted raw data over unsecured channel during signal transmission. This paper tried to contribute to the general body of knowledge in the area of cryptography by analyzing various algorithms which make use of the concept of hybrid cryptography. It can be concluded that in spite of the increased computational complexity, cryptographic goals such as confidentiality, integrity and authenticity can be achieved by using hybrid cryptographic approaches.

REFERENCES