IJCAT - International Journal of Computing and Technology, Volume 3, Issue 2, February 2016
ISSN : 2348 - 6090
www.IJCAT.org

A Survey on Various Encryption Cryptographic Techniques

[1] **Ritu Patidar,** [2] **Rupali Dave,** [3] **Anubha Sharma**

[1, 2, 3] Assistant Professor, Department of Computer Science,
RGPV University, SVITS,
Indore, India

Abstract - In modern era, it should be noted that all work related to banking, ATM card, credit card, marketing, E-commerce etc are done on internet. So there must be security provided over the network. In this paper we survey the researches held on various encryption methods used in cryptography and attacks such as factorization problem, low decryption exponent, common modulus, short message, cyclic attack and side channel attack etc. This paper presents the theoretical aspects and comparative study about different encryption techniques in cryptosystem.

Keywords **- RSA algorithm, encryption, decryption, public key, private key, prime number theorem(PNT) , C4,Greatest Common Divisor(GCD).**

1. Introduction

Today's world, the security for the data has become highly important since the communication by transmitting of digital products over the open network occur very frequently , it should be noted that all work related to banking, atm card, credit card, marketing, Ecommerce etc are done on internet. So there must be security provided over the network. Therefore for secure communication we have many cryptography technique used like hash function, diffie hellman, digital signature, message authentication code, MD5 algorithm, Rabin cryptosystem, RSA etc.

We apply these techniques to secure information in order to provide confidentiality from an unauthorized access. Large volume of Personnel and sensitive information are electronically transmitted and stored every day. In cryptosystem data are secured through encryption method for making communication private. Anyone to send the private message by encrypt the message and intended receiver decrypt it by its key. Every encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security.

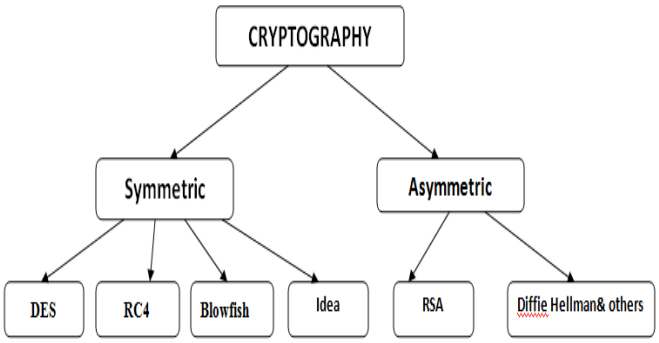

Figure 1.1-Symmetric and Asymmetric cryptographic techniques

1.1 RSA Methodology

In public cryptosystem, the common and most important public key algorithm is RSA cryptosystem .The security of RSA is based on factoring a large number. If we determined the factors of large prime numbers then the whole algorithm can become breakable.RSA is commonly used public key cryptosystem which was discovered by Rivest, Shamir and Adelman in 1977 at MIT. It is an asymmetric public key algorithm in which it uses two exponents 'e' and 'd' where e is public and d is private key. It is based on three steps such that-Encryption phase, Key generation and Decryption phase.RSA uses modulus exponentiation for encryption and decryption. To be secure, the recommended size for each prime, p or q, is 512 bits (almost 154 decimal digits) and the size of n modulus are 1024 bits (309 digits)Its security based on large prime numbers because it is not easy to factor a large prime number.

Let's consider how keys are generated in RSA cryptosystem:-

- Key Generation

Step1. Select p, q where p and q both prime , p is not equal to q

Step2. Calculate n = p xq.

Step3. Calculate Ø(n) = (p -1) x (q-1)

Step4. Select integer e whose gcd (Ø (n), e) = 1; 1 < e < Ø(n).

Step5.Calculate d d = e-1 (mod Ø(n)).

Step6. Public key PU = {e,n}.

Step7. Private key PR = {d,n}

- Encryption Process

Plain text : M < n
Cipher text: C = M^e mod n

- Decryption process

Cipher text:
Plain text: M = C^d mod n.

1.2 Attacks on RSA

- **Factorization Attack**

Prime numbers are play an important role in RSA to provide more over the communication network because it is very difficult to decompose a large integer into its prime constituents. In RSA we use n prime numbers which is not easily breakable. It uses composite number N whose factors are not known. Today's the most promising method is to solving the factors problem in RSA.If attacker are recovered the value prime factor then it can break the whole cryptosystem by using traditional RSA method. There are various factorization algorithm now A days but none of them can factor a large integer in polynomial time p(n).If we use the largest and fastest computer to solve this problem it take too much time to compute and it infeasible. Therefore RSA is as secure as an efficient algorithm has not been developed to make the factors. The solution of this problem is solved in many research papers by applying some mathematical theorems such that prime number theorem (PNT) and Euclid's theorem.

PNT: - This theorem provides the asymptotic distribution of prime numbers. It gives a general description how the prime numbers are distributed among the positive integers. In PNT random number is selected in the range of zero to some large integer N. the probability that the selected integer is prime is about $1 / \ln(N)$, where $\ln(N)$ is the natural logarithm of N.

1.3 Attacks on Encryption Exponent

To reduce the encryption time it is easier to use small value of public encryption exponent e in RSA. Therefore we use a common value of e is 3.There are several attacks on encryption exponent such as

1.3.1 Low Encryption Exponent Attack

Low encryption attack is also referred as coppersmith attack. It states that in modulo n polynomial f(x) of complexity log n to find roots whose value is smaller than n^1/e. this theorem can be applied to RSA cryptosystem with C=f(p)=P^emodn.If e=3 and only 2/3 of bits in P is known the algorithm can find the original bits in plaintext. This problem is solved by coppersmith theorem and LLL lattice reduction algorithm applies on RSA to find the roots of low degree polynomial.

1.3.2 Broadcast Attack

Broadcast attack happened when an entity sends the same message to a group of recipients with same encryption exponent e. If any entity wants to send the same message to three or more recipients with same public exponent e=3 and modulo n1, n2,n3 then after encryption we get:-

C1= P^3modn1

C2= P^3modn2

C3=P^3modn3

Applying Chinese remainder theorem (CRT) ti these equations, anyone can find an equation of the form C'=P^3MODn1n2n3. Therefore we can easily compute P from cipher text. So the security of RSA can break if any unauthorized person can see this message P.

1.3.3 Short Pad Attack

Short pad attack is discovered by coppersmith can be briefly described as follows:-

1. If an entity A has a message M to send to an Entity B.
2. Entity A pads the message with r1,encrypt the result to get cipher text C1 and send C1 to entity B.

3. Any unauthorized person E intercept C1 and drop it

4. Entity B informs Entity A that the he has not received the messages ne entity A pads the message again and encrypts with r2 and send C2 t o B.

5. Then again an unauthorized person E is also intercepts this message.

6. Therefore E have both C1 and C2.It knows that both are cipher text belong to same plaintext.

7. Coppersmith proved that if r1 and r2 are too short, then person E may be able to recover the original message from cipher text C1.

1.4 Attacks on Decryption Exponent

1.4.1 Common Modulus Attack

It is an obvious attack occurs on RSA cryptosystem. Anyone who is an eavesdropper on the communication system can easily see the message if it is able to found the common modulus n. The common modulus can occurred if an organization or any group uses a common modulus n.RSA implementation gives to everyone the same n, but different values for exponent e and d.

The problem is that if the same message is encrypted with two different exponent (e ,d having same modulus) and those two exponent are relatively primes are distributed among the group. Any unauthorized person in that group can recovered the plaintext without either of decryption exponent. This attack can overcome by modifying the existing RSA algorithm.

To avoid this we used change modulus value will be publically announced which are fake value f (n)in place of n. If any unauthorized person are try to factorize it cannot get the new modulus value and decryption key (d).Therefore this overcome the weakness of factor the n.

1.4.2 Low Decryption Attack

This problem states that in RSA cryptosystem with small secret decryption exponent d, which works if d<n^0.25, Where n=pq is the modulus in RSA. It is polynomial time attack. To increase the speed of RSA we used small secret value of d..It is reliable to work if two communicating parties have large difference in their computing power for example communication between computer and smart card.

2. Advanced Encryption Standard (AES)

AES consist of three block ciphers named AES-128, AES-192 and AES-256. In a cryptography, symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key .There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys . A round comprises of a few handling steps that incorporate substitution, transposition and blending of the input plaintext and changes it into the last yield of cipher text. It depends on substitution–permutation system. It includes a progression of connected operations, some of which include replacing inputs by particular yields (substitutions) and others include rearranging bits around (permutations).

- Encryption Process

Byte Substitution (Sub Bytes)

There 16 data bytes are substituted by alludes a settled table (S-box) given in configuration. The outcome is in a network of four lines and four segments.

Shift Rows

Each of the four columns of the network is moved to one side.

Mix Columns

Every segment of four bytes is currently changed utilizing a mathematical function. This function takes as information the four bytes of one segment and produces four totally new bytes, which replace the original column. The outcome is another new matrix comprising of 16 new bytes. It ought to be noticed this stride is not performed in the last round.

Add Round Key

The 16 bytes of the grid are currently considered as 128 bits and are XORed to the 128 bits of the round key. On the off chance that this is the last round then the yield is the cipher text. Something else, the subsequent 128 bits are deciphered as 16 bytes and we start another comparative round.

- Decryption Process

The procedure of decryption of an AES cipher text is like the encryption process in the converse order. Each round

comprises of the four procedures led in the converse order –

- Include round key
- Mix sections
- Shift rows
- Byte substitution

Since sub-forms in each round are backward way, dissimilar to for a Feistel Cipher, the encryption and unscrambling calculation should be independently implemented, despite the fact that they are firmly related.

It is a block cipher framework which changes 64-bit information block under a 56-bit mystery key under a 56-bit secret key, by method for permutation and substitution. Every block is enciphered utilizing the secret key into a 64-bit cipher text by method for permutation and substitution. The procedure includes 16 rounds and can keep running in four unique modes, encoding blocks separately or making every cipher block dependent on all the previous blocks. Decryption is just the backwards of encryption, taking after the same steps yet switching the request in which the keys are connected.

For any block, the most fundamental system for attack is brute force, which includes attempting every key until you locate the right one. The length of the key decides the number of possible keys and henceforth the achievability of this sort of attack.

3. Data Encryption Standard (DES)

3.1 DES Algorithm

- Fractioning of THE TEXT

  Fractioning of the text into 64-bit (8 octet) blocks.

- Initial Permutation

  Firstly, each bit of a block is subject to initial permutation, which can be represented by the following initial permutation (IP) table.

- Division into 32-bit blocks

  Once the initial permutation is consummated, the 64-bit block is divided into two 32-bit blocks, respectively denoted L and R (for left and right). The initial status of these two blocks is denoted L0 and R0.

- Rounds

  The Ln and Rn blocks are subject to a set of reiterated transformations called rounds, shown in this diagram, and the details of which are given below:

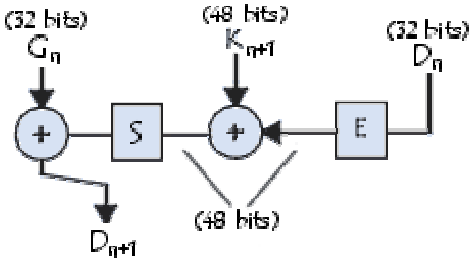

Figure 3.1- Data encryption standard diagram (permutation and substitution)

- Expansion Function

The 32 bits of the $\mathbf{R}_0$ block are expanded to 48 bits thanks to a table called an expansion table (denoted **E**), in which the 48 bits are mixed together and 16 of them are duplicated.

- Exclusive OR with The Key

The resulting 48-bit table is called $\mathbf{R'}_0$ or $\mathbf{E}[\mathbf{R}_0]$. The DES algorithm then exclusive ORs the first key $\mathbf{K}_1$ with $\mathbf{E}\ [\mathbf{R}_0]$. The result of this exclusive OR is a 48-bit table we will call $\mathbf{R}_0$ out of convenience (it is not the starting $\mathbf{R}_0$).

- Substitution Function

$\mathbf{R}_0$ is then divided into 8 6-bit blocks, denoted $\mathbf{R}_{0i}$. Each of these blocks is processed by **selection functions** (sometimes called substitution boxes or compression functions), generally denoted $\mathbf{S}_i$.

- Exclusive OR

All of these results output from **P** are subject to an Exclusive OR with the starting $\mathbf{L}_0$ (as shown on the first diagram) to give R1, whereas the initial $\mathbf{R}_0$ gives $\mathbf{L}_1$.

- Iteration

All of the previous steps (rounds) are repeated 16 times.

- Inverse initial permutation

At the end of the iterations, the two blocks $\mathbf{L}_{16}$ and $\mathbf{R}_{16}$ are re-joined, then subject to inverse initial permutation

- Generation of Keys

Given that the DES algorithm presented above is public, security is based on the complexity of encryption keys.

The algorithm below shows how to obtain, from a 64-bit key (made of any 64 alphanumeric characters), 8 different 48-bit keys each used in the CRYPTOSYSTEM.

4. Rivest Cipher (RC4)

The RC4 Encryption Algorithmic program, developed by Ronald Rivest of RSA, is a shared key flow cipher algorithmic rule requiring a secure substitution of a shared key. The symmetric key algorithm is used identically for encryption and decryption such that the information watercourse is simply XORed with the generated key . The algorithm is serial as it requires successive exchanges of DoS entries based on the key sequence. A variable key-size cipher with byte -oriented operations. The algorithm is based on the use of a random permutation and is commonly used for the encryption of traffic to and from secure Web sites using the SSL protocol. The algorithm uses a variable length key from 1 to 256 byte to initialize a 256-byte United States Department of State table. The state table is used for subsequent generation of shammer - random bytes and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text. Each component in the state table is barter at least once.

- Strength of RC4
  - The difficulty of knowing where any value is in the table.
  - The difficulty of knowing which location in the table is used to select each value in the sequence.
  - A particular RC4 Algorithm key can be used only once.
  - Encryption is about 10 times faster than DES.
- Limitation of RC4

One in every 256 keys can be a weak key. These keys are identified by cryptanalysis that is able to find circumstances under which one of more generated bytes are strongly correlated with a few bytes of the key.

5. Blowfish

Blowfish is a symmetric block cipher, designed by Bruce Schneier. Blowfish is one of the fastest block ciphers in widespread use, except when changing keys. Each new key requires pre-processing equivalent to encrypting about 4 kilobytes of text, which is very slow compared to other block ciphers.

Blowfish has a 64-bit block size and a key length of anywhere from 32 bits to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes. It is similar in structure to CAST-128, which uses fixed S-boxes.

6. International Data Encryption Standard (IDEA)

IDEA encryption algorithm is the European counterpart to the DES encryption algorithm. IDEA is a block cipher, designed by Dr. X. Lai and Professor J. Massey. It operates on a 64-bit plaintext block and uses a 128-bit key. IDEA uses a total of eight rounds in which it XOR's, adds and multiplies four sub-blocks with each other, as well as six 16-bit sub-blocks of key material.

7. Comparative Study Between Different Encryption Techniques

Following are the comparison table between AES (Advanced Encryption Standard), DES (Data Encryption Standard) and RSA Cryptography is described on the basis of literature survey has been done by researchers.

Table 7.1-Comparision table for different encryption techniques

Characteristics	**AES**	**RSA**	**DES**
Key Size	128,192,256 bits	1024 bits	56 bit
Key Used	Public and private keys are used for encryption and decryption of data	Same keys are used for encryption and decryption of data	Same keys are used for encryption and decryption of data
Security	Secure for both provider and user.	Secure for user only	Secure for both provider and user.

Memory Usage	Low RAM needed	Highest memory usage algorithm	More than AES
Execution Time	Faster than others	Require s maxim um time	Equals to AES
Initial Vector Size	128 bits	1024 bits	64 its

8. Conclusion

In this paper comparative study of different encryption algorithms are presented. With theoretical aspects it was concluded that the advanced encryption standard, RSA public cryptography is more efficient than the Data encryption standard. AES can be used when high security is needed. This paper presents the theoretical analysis of selected symmetric algorithms. These selected algorithms are AES, DES, Blowfish, IDEA and RSA. All encryption techniques are discussed and analyzed the working performance of the encryption methods. This paper presents survey on the existing works of the encryption techniques and also presents various attacks in cryptosystem. Each technique of encryption is different in working, which might be suitable for different applications. All the techniques are useful for real-time encryption.

References

[1] Mandeep kaur and Manish Mahajan "Using encryption Algorithms to enhance the Data Security in Cloud Computing", International Journal of Communication and Computer Technologies Vol.01 – No.12, Issue.03, January 2013.

[2] Prof.Dr. Alaa Hussein Hamamiand, Ibrahem Abdallah Aldariseh, "Enhanced Method for RSA Cryptosystem Algorithm", International Conference on Advanced Computer Science Applications and Technologies, pp.402-408, Nov 2012.

[3] XinZhou and Xiaofei Tang "Research and Implementation of RSA Algorithm for Encryption and Decryption", The 6th International Forum on Strategic Technology, Vol.2, pp.1118-1121, Aug 2011.

[4] Sami A. Nagar and Saad Alshamma "High Speed Implementation of RSA Algorithm with Modified Keys Exchange", 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT), pp.639-642, March 2012.

[5] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Vol. 21, pp.120-126, 1978.

[6] W. Stallings "Cryptography and network security", vol. 2 prentice hall, 2003.

[7] Ravi Shankar Dhakar and Amit Kumar Gupta "Modified RSA Encryption Algorithm (MREA)", Second International Conference on Advanced Computing & Communication Technologies, pp.426-429, Jan 2012.

[8] B.Persis Urbana Ivy, Purshotam Mandiwa. Mukesh Kumar "A modified RSA cryptosystem based on 'n' prime numbers", International Journal Of Engineering And Computer Science, Vol.1, pp. 63-66, 2 Nov 2012.

[9] Shilpi Gupta and Jaya Sharma "A hybrid encryption algorithm based on RSA and diffie hellman", IEEE International Conference on Computational Intelligence and Computing Research, pp.1-4, Dec 2012.

[10] Wuling Ren and Zhiqian Miao, "A hybrid encryption algorithm based on DES and RSA in Bluetooth communication", Second International Conference On Modeling, Simulation and Visualization Methods, pp. 221-225, May 2010.

[11] [1] William Stallings " Network Security Essentials (Applications and Standards)", Pearson Education, 2004.