Comparative analysis and Evaluation of RC6, Blowfish, IDE, CAST-128 and DES Algorithms.

Mohammad Saleem Bari*1, Ahmad TalhaSiddique*2

M.Tech Student Dept. of CS&IT, MaulanaAzad National Urdu University, Hyderabad, India.

Ahmad Talha Siddique. Assistant Professor, Dept. of CS&IT, Maulana Azad National Urdu University, Hyderabad, India

Abstract: Quick development of web applications powered the requirement for securing data and PCs. Encryption calculations assume essential part to secure data. Digital security guarantees a safe data trade and empowers correspondence through the Internet. The information should be shielded from unapproved access and transmitted to the planned recipient with secrecy and trustworthiness. Cryptography upgrades security by encoding and decoding crude information in a secured organize. Numerous cryptographic calculations are accessible, and they fall under either symmetric or topsy-turvy strategies. To pick a calculation for secure information correspondence, the applicant calculation ought to give higher precision, security and proficiency. This paper shows the execution constraints of existing cryptographic calculations, for example, DES, 3DES, CAST-128, BLOWFISH, IDEA, AES, and RC6 of symmetric methods and RSA of lopsided procedures. DES, IDEA, Blowfish, CAST-128 has square size of 64 bits. DES has key Size of 64 bits while Blowfish,IDEA,CAST-128 has key size 128 bits. The RC6 has Key size and Block size of 128 bits. Simulation comes about are given to show the viability of every calculation.

Keywords: Cryptography, Symmetric encryption, DES, Blowfish, CAST-128, RC6, IDEA.

1. Introduction: Cryptography is a procedure which is expected to change the information and can be utilized to give different security related ideas, for example, classification, information uprightness, authentication, approval and non-disavowal. It relies upon two essential components: a calculation and a key. The calculation is a numerical method and the key is a factor utilized for information change. These calculations give cryptographic assurance to the information by utilizing encryption and the switch by decryption. These calculations can be Symmetric key Algorithms or Asymmetric key calculations. Symmetric calculations (Secret Key Algorithms) utilize a solitary key for both encryption and unscrambling. Numerous encryption calculations are accessible which can be ordered as symmetric key encipherment and lopsided key encipherment. Symmetric key encipherment includes one key which is utilized for both encryption and decoding. Uneven key encipherment utilizes diverse keys for encryption and decoding.

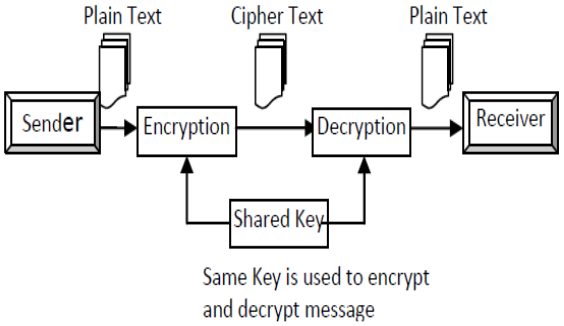
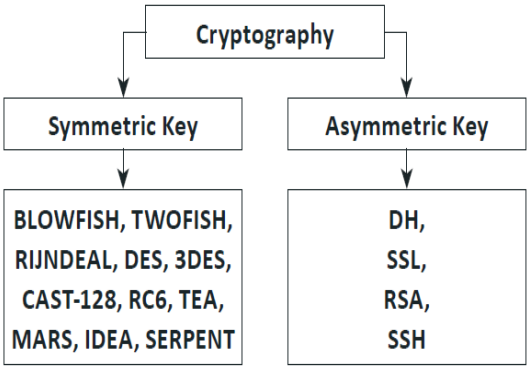


Fig 1. Symmetric encryption and decryption

The essential grouping of cryptographic calculations is appeared in Figure 1. Many creators have analyzed these calculations based on time intricacy and space multifaceted nature. This paper thinks about these calculations depends on parameters like key length and administration, security and constraints relating to every algorithm.



DES:DES takes 64 bit plaintext which makes 64 bit figure content. The core of DES is the DES function.DES work applies a 48 bit key to the furthest right 32 bits to deliver a 32 bit yield. This capacity is comprised of four operations: a development change, a whitener, a gathering of S boxes and a straight stage. DES is currently thought to be shaky for some applications. This is mostly due to the 56-bit key size being too little.

Blowfish: Blowfish is a keyed, symmetric square figure, planned in 1993 by Bruce Schneier. Schneier composed Blowfish as a universally useful calculation, planned as a contrasting option to maturing DES. Blowfish has a 64-bit piece measure and a variable key length from 32 bits up to 448 bits. 18 sub-keys are gotten from a solitary starting key. It requires add up to 521 emphases to produce all required sub keys. It is a 16-round Feistel figure and uses vast key-subordinate S-boxes. In structure it looks like CAST-128, which utilizes settled S-boxes. Blowfish performs well for applications in which keys does not change frequently.

CAST-128: CAST-128 is a 12 or 16-round Feistel connect with a 64-bit square size and key size of 40 to 128 bits. The full 16 rounds are utilized when the key size is longer than 80 bits. Parts incorporate expansive 8×32-piece S-boxes in light of bowed capacities, key-subordinate revolutions, particular expansion and subtraction, and XOR operations. There are three rotating kinds of round capacity, however they are comparative in structure and vary just in the decision of the correct operation at different focuses. Despite the fact that Entrust holds a patent on the CAST plan methodology, CAST-128 is accessible worldwide on an eminence free reason for business and non-business employments.

RC6 :RC6 is a piece figure in view of RC5 and planned by Rivest, Sidney, and Yin for RSA Security. Like RC5, RC6 is a parameterized calculation where the square size, the key size, and the quantity of rounds are variable; once more, as far as possible on the key size is 2040 bits. RC6 was intended to meet the necessities of the Advanced Encryption Standard (AES) rivalry. RC6 appropriate has a square size of 128 bits and backings key sizes of 128, 192 and 256 bits.At the

same time, as RC5. RC6 can be seen as intertwining two parallel RC5 encryption forms. It utilizes an additional duplication operation not present in RC5 keeping in mind the end goal to make the turn reliant on each piece in a word.

IDEA: Universal Data Encryption Algorithm is a piece figure composed by James Massey of ETH Zurich and Xuejia Lai and was first portrayed in the year 1991. The calculation was proposed as a substitution for the Data Encryption Standard. Thought is a minor update of a prior figure, Proposed Encryption Standard.IDEA was initially called Improved PES. Thought works on 64-bit pieces utilizing a 128-piece key and comprises of a progression of eight indistinguishable changes and a yield change.

2. DES (Data Encryption Standard):

DES is a calculation that takes a settled length string of plaintext bits and changes it into content piece string of the similar length. The account of DES, the piece measure is 64 bits. The DES additionally utilizes a key to redo the changes. The key comprises of 64 bits, in any case a just 56 of these are really utilized by the calculation. Eight bits are utilized exclusively to check equality and are from there on disposed of.

2.1 Key Generation

At first, 56 bits of the key are chosen from the underlying 64 by Permuted Choice 1 (PC-1) the staying eight bits are either disposed of or utilized as equality check bits. The 56 bits are then partitioned into two 28 bit parts; In this every half is from that point treated independently. In progressive rounds, the two parts are turned left by maybe a couple bits and after that 48 subkey bits are chosen by Permuted Choice 2, 24 bits from the left half and 24 from the right.

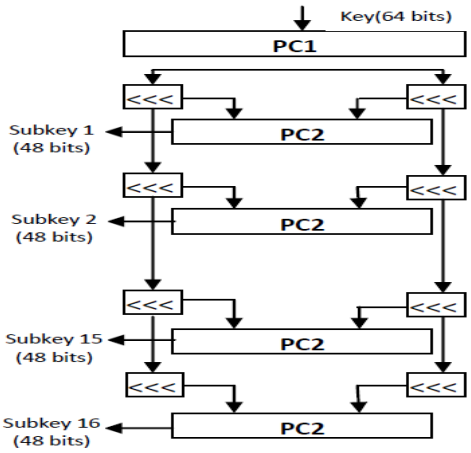


Fig 2. DES Key Generation

The ⊕ symbol denotes the exclusive-OR operation. The F-work scrambles a large portion of a piece together with a portion of the key. The yield from the F-work is then joined with the other portion of the square, and the parts are swapped before the following round. After the last round, the parts are swapped; this is a component of the Feistel structure which makes encryption and unscrambling comparable procedures.

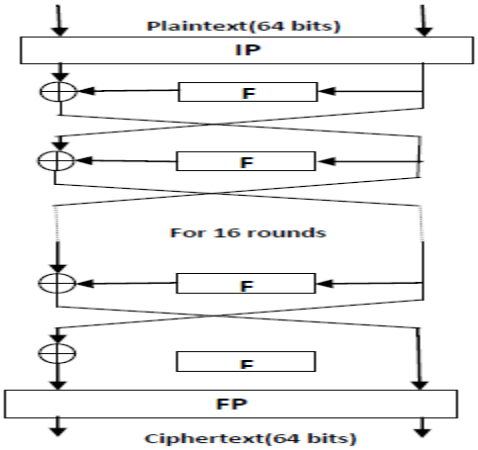


Fig 3. DES Encryption and Decryption

3. BLOWFISH

It is appropriate for applications where the key does not change frequently, similar to correspondence

connect record encrypted. Blowfish symmetric square figure calculation encodes piece information of 64-bits at once. It takes after the feistel system and this calculation is divided into two parts. They are Keyage and Data Encryption.

3.1 Key Generation

Blowfish utilizes a substantial number of sub keys. These keys must be pre figured before any information encryption or unscrambling.

The P-array consists of 18 32-bit subkeys:

P1, P2,..., P18.

There are four 32-bit S-boxes with 256 entries each:

S1,0, S1,1,...., S1,255;

S2,0, S2,1,...., S2,255;

S3,0, S3,1,....., S3,255;

S4,0, S4,1,...., S4,255.

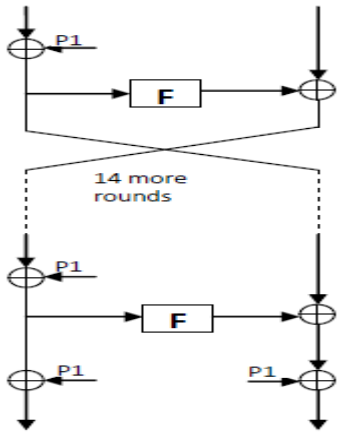


Fig 4: The Feistel structure of Blowfish

3.3 Decryption

Decryption is exactly the same as encryption, except that P1, P2…P18 are used exactly in reverse order.

4. CAST-128

CAST has a classical Feistel network contains 16 rounds and operating on 64-bit blocks of plaintext to produce 64-bit blocks of cipher text. The key size generally varies from 40 bits to 128 bits in 8-bit increments.

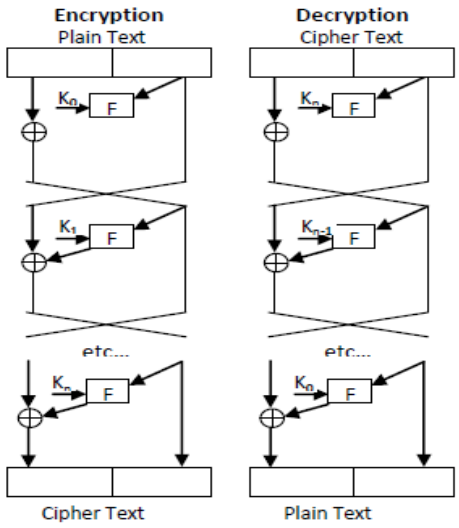


Fig 5. Cast-128 Encryption and Decryption

5. RC6

RC6 is a completely parameterized group of encryption calculations. An adaptation of RC6 is all the more precisely determined as RC6-w r b where the word measure is w bits and encryption comprises of a nonnegative number of rounds r, and b indicates the length of the encryption enter in bytes. Since the AES accommodation at w = 32 and r = 20, we might utilize RC6 as shorthand to allude to such forms. At the point when some other estimation of w or r is expected in the content, the parameter esteems will be indicated as RC6-w r. Of specific significance to the AES exertion will be the forms of RC6 with 16-, 24-, and 32-byte keys.

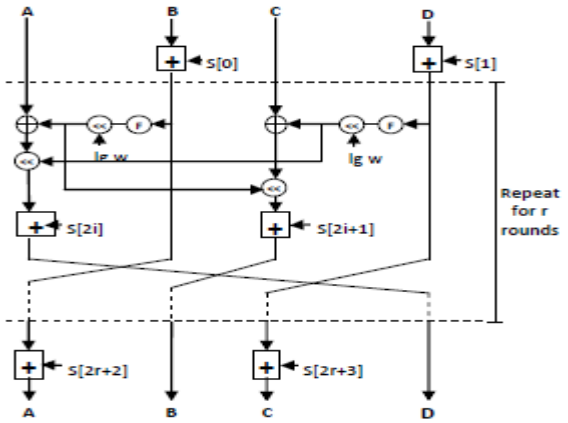


Fig 6. RC6 Encryption

6. IDEA

Thought works on 64-bit squares utilizing a 128-piece key, and comprises of a progression of eight indistinguishable changes and a yield change. The procedures for encryption and decoding are comparative.

6.1 Encryption and Decryption

For each of the eight finish adjusts, the 64-bit plaintext square is part into four 16-bit sub-pieces: X1, X2, X3, X4. The 64-bit input square is the link of the sub pieces:

X1 || X2 || X3 || X4, where || indicates link. Each entire round requires six sub keys. The 128-piece enter is part into eight 16-bit squares, which end up noticeably eight sub keys. The initial six sub keys are utilized as a part of cycle one and the staying two sub keys are utilized as a part of cycle two.

Each round utilizations each of the three arithmetical operations: bitwise XOR, expansion modulo 2^{16}, and duplication modulo $2^{16} + 1$.

6.2 Key Scheduling

Each of the eight finish rounds requires six sub keys, and the last change "half round" requires four sub keys; in this way, the whole procedure requires 52 sub keys. The 128-piece enter is part into eight 16-bit sub keys which shapes the initial 8 sub keys. At that point the bits are moved to one side 25 bits. The subsequent 128-piece string is part into eight 16-bit obstructs that turn into the following eight subkeys. The moving and part process is rehashed until 52 subkeys are created. The movements of 25 bits guarantee that reiteration does not happen in the sub keys. Six sub keys are utilized as a part of each of the 8 rounds. The last 4 sub keys are utilized as a part of the ninth "half round" conclusive change.

Correlation of Cryptographic Algorithms in view of different Parameters:

Among the many existing cryptographic calculations, DES, 3DES, CAST-128, BLOWFISH, IDEA, AES, RC6 and RSA are chosen and analyzed based on structure, security, adaptability to grow in future and confinements. Table 1 represents the similar investigation on chose calculations.

Algorithm	Structure	Flexibility and Modification	Known Attacks
DES	Feistel	NO	Brute Force Attack
3DES	Feistel	YES, Extended from 56 to 168 bits	Brute Force Attack, Chosen Plaintext, Known Plaintext
CAST-128	Feistel	YES, 128 and 256 bits	Chosen Plaintext Attack
BLOWFISH	Feistel	YES, 64-448 key length in multiplies of 32	Dictionary Attack
IDEA	Substitution-Permutation	NO	Differential Timing Attack, Key-Schedule Attack
AES	Substitution-Permutation	YES, 256 key length in multi-ples of 64	Side Channel Attack
RC6	Feistel	YES, 128-2048 key length in multiples of 32	Brute Force Attack, Analytical Attack
RSA	Factorization	YES, Multi Prime RSA, Multi power RSA	Factoring the Public Key

Table 1: Qualitative measures

Security in cryptography depends on how secure the calculation is against different attacks. The execution of these cryptographic calculations depend on structure, key length, piece estimate, number of rounds utilized, and cryptographic time. At last, these are the components which influences

the security of a specific calculation. The piece measure assumes a fundamental part in encryption and unscrambling, which is the essential unit of information.

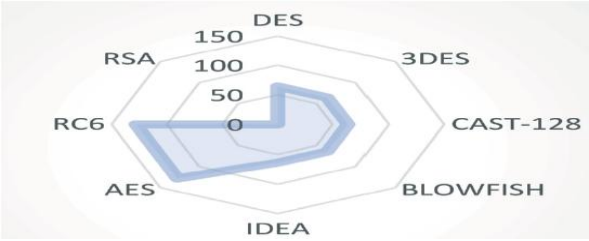


Figure 2: Quantitative measures – Block Size (Bits)

Bigger square size gives higher security when different variables were thought to be equivalent in a few calculations. AES utilizes square size of 128 bits which is twice greater than all other symmetric calculations in exchange. Another basic assessment is on number of rounds utilized for encryption/decoding process.

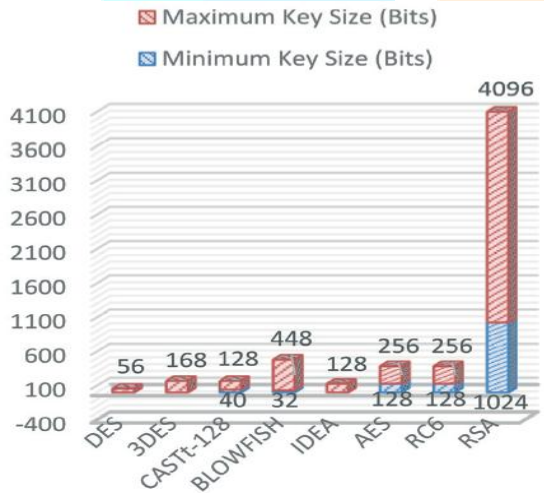
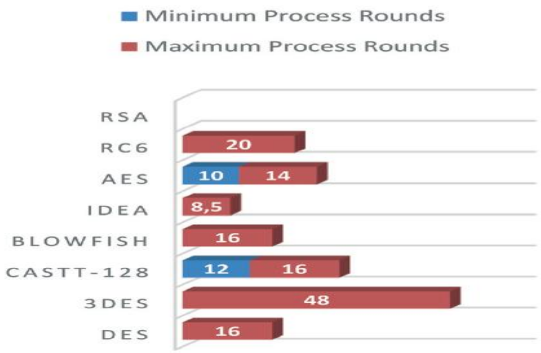


Figure 3: Quantitative measures – Key Size (Bits)

Increment in handling rounds, reinforces the security as single Feistel round gives lacking security. DES and BLOWFISH has 16 rounds of process. 3DES has 3 times of DES (48 rounds). AES has shifting number of rounds depending of key size. RC6 is the best applicant which has 20 rounds of process with respect to as this rule is concerned. The significant issue with symmetric key calculations is a savage power assault, where all conceivable keys are attempted until the point when the correct key is found to unscramble the message. Longer key lengths decrease the practicality of assaults, since the quantity of key blends increment.



DES has a frail key of 56 bits. CAST-128, IDEA utilize 128 bits key which is thought to be normal key quality. 3DES has 168 bits key with great protection against assault. RC6 and AES has variable key lengths of 128, 192, and 256 which give a bigger number of key blends. BLOWFISH utilizes 448 piece keys which are thought to be longest and most grounded the extent that beast constrain assaults are concerned. In lopsided RSA, a key trade isn't required and this expands the security of the calculation. RSA utilizes factorization for the cryptographic procedure which altogether reduces the speed of the calculation. Symmetric calculations like AES, BLOWFISH, and RC6 are significantly quicker than RSA. Security of the cryptosystem is characterized by a secured encryption plan to make preparations for animal power assaults and differential plaintext figure content assault. In spite of the fact that CAST-128, IDEA, DES, 3DES are speedier, they are less

secure because of powerless keys. The investigation appears if there should arise an occurrence of symmetric calculations RC6, Blowfish and AES that they are thought to be secure and productive in light of high security and less restrictions. The expansion and adaptability of RC6, Blowfish and AES are high contrasted with other symmetric calculation. The correlation of symmetric and topsy-turvy keys demonstrate that RSA is more secure than any symmetric cryptographic calculation.

Conclusion: This paper gives a diagnostic investigation on different symmetric encryption calculations, for example, DES, 3DES, CAST-128, BLOWFISH, IDEA, AES, RC6 and deviated RSA Algorithm. The investigation depends on the engineering of the calculations, the security viewpoints and the constraints they have. The examination unmistakably expresses that however awry algorithms are prevalent in security, they set aside more opportunity for handling and requires more memory. For all intents and purposes, unbalanced calculations like RSA are utilized for the key trade and symmetric calculations are utilized for encryption/unscrambling. general implementation restrictions of cryptographic calculation accentuation the choice amongst equipment and programming cryptosystem, picking among symmetric and deviated key calculation and the fundamental variables to be taken after to have a safe key administration. Effective cryptosystems can be given by applying more than one calculation as a cross breed cryptosystem which gives high security and secure information exchange.

References:

[1] Ronald L. Rivest,"THE RC6 Block Cipher" RSA Laboratories, 2955 Campus Drive, Suite 400, San Mateo, CA 94403, USA.

[2] IDEA "wikipedia.org**".** Available at: http://en.wikipedia.org/wiki/International_Data_ EncryptionAlgorithm

[3] "What are RC5 and RC6","rsa.com". Available at: http://www.rsa.com/rsalabs/node.asp.

[4] B. Schneier, **"**Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)",Available at: http://www.schneier.com/paper-blowfish-fse.html

[5] B. Schneier, "Applied Cryptography", John Wiley & Sons Inc., 1999

[6] Harsh Kumar Verma, and Ravindra Kumar Singh, "Performance Analysis of RC5, Blowfish and DES Block Cipher Algorithms", International Journal of Computer Applications (0975– 8887) March 2012 Volume 42– No.16.

[7] Joseph, D. P., Krishna, M. and Arun, K. (2015). Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms.International Journal of Advanced Re-search in Computer Science, vol. 6, no. 3.

[8] Mandal, A. K., Parakash, C. and Tiwari, A. (2012). Performance evaluation of cryptographic algorithms: DES and AES. Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on.IEEE, 2012.

[9] Nadeem, A. and YounusJaved, M. (2005). A performance comparison of data encryption algorithms.Information and communication

technologies, 2005.ICICT 2005.First international conference on.IEEE.

[10] Salama, D. et al. (2008). Performance Evaluation of Symmetric Encryption Algorithms.

[11] William, S. (1999). Cryptography and network security: principles and practice, pp. 23-50, Prentice-Hall, Inc.

[12] Agrawal, M. and Mishra, P. (2012). A comparative survey on symmetric key encryption techniques.International Journal on Computer Science and Engineering, vol. 4, no. 5, p. 877.

[13] Apoorva, Y. K. (2013). Comparative study of different symmetric key cryptography algorithms.International Journal of Application or Innovation in Engineering and Management,
vol. 2, no. 7, pp. 204-6.

[14] Arora, S. (2015). Enhancing Cryptographic Security using Novel Approach based on Enhanced-RSA and Elamal: Analysis and Comparison. International Journal of Computer Applications,vol. 112, no. 13.

[15] Daemen, J. and Rijmen, V. (1999). AES Proposal: Rijndael. AES Algorithm Submission, September3, http://www. nist.gov/CryptoToolKit.

About Authors:

Mohammad Saleem Bari M.Tech(CS), B.Tech (IT) mtech931517@gmail.com

Student M.tech, Department of CS&IT, Maulana Azad National Urdu University, Hyderabad, India

Ahmad Talha Siddique, Mtech (CS), ahmedtalha207@gmail.com, Assistant Professor, Department of CS&IT, Maulana Azad National Urdu University, Hyderabad, India

Published International Journal Papers:8
Conference Proceedings (Published:5)
Conference/Workshop Attend: 2

.