ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(38), DOI: 10.17485/ijst/2016/v9i38/98035, October 2016* ISSN (Online) : 0974-5645

A Survey on Crypt- Algorithms in Voting System

P. Ashok[1*], P. Annadurai[1], R. Lavanya[2] and P. Raghuvara Pandian[3]

[1]Department of Computer Science and Engineering, Sri Sai Ram Institute of Technology, Chennai - 600044, Tamil Nadu, India; ashokit009@gmail.com, durai.ebe@gmail.com
[2]Department of Information Technology, E. G. S. Pillay Engineering College, Nagapattinam - 606611, Tamil Nadu, India; lavanya.ngpt@gmail.com
[3]Department of Computer Science and Engineering, Adhi College of Engineering and Technology, Walajabad - 601206, Tamil Nadu, India; raghuvarapandiyan@gmail.com

Abstract

Objectives: Traditional voting process held at polling booths have been changed by merging technologies. Though voting system changed, the security provided was unfit to use it in real time. Thus this paper shows the result analysis of various crypt-algorithms to provide more security for voting process. **Methods/Statistical Analysis:** File Size, Upload & Download time, Efficiency, Memory usage, Speed, Throughput of various Crypt-Algorithm such as AES, RSA, ECC, Visual Cryptography, Blowfish were considered, compared and analyzed. So, we can obtain a better Crypt-Algorithm for Voting. **Findings:** A suitable Crypt-Algorithm for security which can give good performance in parameters like throughput, Average speed, etc.., was obtained in this survey. **Application/ Improvement:** Local Election, Data Transferred over network will be secure for various applications, useful for e-commerce software, used to secure passwords.

Keywords: Android System, AES, Blowfish, Security, Vote

1. Introduction

The development in technologies makes the world to turn impossible to possible in real-time. By this improvement in modern world, the various new developments in traditional system have made. One of them is mobile phone. Across the globe, about 9.4 billion mobile phones users are found. The usage of mobile phones not only ends with calling and messaging, but also includes internet banking, purchasing, emailing and so on. In that way, using mobile phones for voting can also be done to make the voting process easier. Election is the way for choosing their leader to govern people. Paper ballot for voting is one of the traditional methods. Electronic voting Machine was used later to vote using electronic devices which consists of a control unit and a ballot unit. The votes casted are recorded and stored for result analysis. Then internet voting is introduced to vote through internet in a remote system. Since android, an open source operating system, developing voting application to vote for election is made easier. Though the technologies have been developed, security is the first demanded thing for votes casted. The development in technologies makes things easier. But less than few milliseconds for hacker is ample to demolish the globe. We must encrypt the confidential data before transmitting them into untrusted network. Thus we need an efficient and powerful cryptographic algorithm to protect the valuable data over internet.

2. Secure Internet Voting System

To avoid problems such as booth capturing, fake votes, duplication of votes, this paper uses visual cryptography to ensure security and voter's privacy. The methodology used this paper to cast vote is, first the voter has to register his/her identity to a central authority through online. On the Election Day, voter login into the android system using given user id and password. After verification, the candidates list is sent to voter. The voter can select their intended candidate. The selection of candidate to vote initiates a vote request to server. On receiving the vote request, the server generates OTP (One Time

* *Author for correspondence*

Password). Digital Signature Algorithm (DSA) which accepts OTP and creates Captcha from the respective OTP. Visual Cryptography (VC) algorithm generates Share on acquired captcha. Captcha (data) is subdivided into a number of shares to construct a secret image. The secret image created is then sent to voter, the voter's device decrypts the image without using any decryption algorithm. After reconstructing the image from shares, the secret data (OTP) is obtained. The voter needs to enter OTP; DSA generates hash value from the data entered. The server compares actual hash value with currently entered hash value. On successful verification, the vote is registered[1]. The cryptographic algorithm used here is visual cryptography (VC) technique (Figure1). In this technique, the information such as text, image, etc., are encrypted. The cipher data is obtained in subdivided 'n' share. The system that acquired all those shares can only be able to obtain the actual data.

Even though 'n-1' shares are obtained, the receiver cannot obtain the actual data sent. The information can be obtained from shares by combining them where the matching black pixels in each share will for a graphical data set.VC aids secret restoring of data without demanding any computation and robust nature. VC also has some negative aspect in security. If one of the shares is averted, the transparency of data will be shifted and pixel expansion becomes an unavoidable drawback. Similarly Smaller sized pixels are harder to align which gives poor resolution than actual data. Colored images demands for additional computation. Some Cheating Intended Visual Cryptographic Systems (CIVCS) are there to which provides duplicate share on reconstruction of data[2]. To avoid the above problems, we go for another cryptographic algorithm.

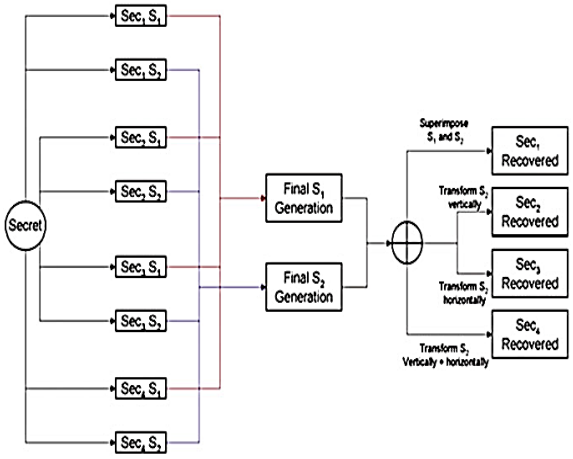

Figure 1. Computation of data in visual cryptography.

3. Overview of the Ivote 2015 Voting System

Methodology used in this paper is that, voter registration is done through online or through Ivote registration call center. After registration voter chooses a PIN and receives an Ivote number through a separate channel which is different from the channel used for registering. This PIN and Ivote number contains voter's secret credentials using which voter will be logged in into the Ivote system to register their vote. On Election Day, voter requests for ballot by entering Ivote number and PIN number[3]. The verification server verifies them and checks voter credentials and provides the voter with requested ballot which is encrypted using Elgamal cryptography algorithm. It was developed by Taher Elgamal as a public key cryptography. It uses the concept of discrete Logarithm. Using the received ballot, the voter can cast their vote. After polling the voter is given with a receipt number to verify whether the vote they casted has been registered or not. The Elgamal algorithm used here is efficient and consumes less power for computation. The main drawbacks of Elgamal algorithm are that it generates cipher text which is more than twice the length of given data, the sender has to select a random integer value for every data, and it works with slower speed. During encryption process, the actual length of plain text is changed and a message is expanded. Elgamal suffers by man-in-middle-attack. Thus to avoid such problems, we go for RSA.

4. E Voting using Android System

In this paper RSA algorithm is used to reduce the size of cipher text and it allows voter to vote through mobile phone. Throughout the voting process, internet facility in the device is essential. The voter needs to register by using voter id, password and photo. The registered voters detail will be store in a database. The voter has to login into the android application in mobile phone using voter id, password and face recognition. For this face recognition Eigen face algorithm is used to check whether the voter is a valid voter or not. After authentication the encrypted ballot is sent to the voter. For encryption RSA, the asymmetric algorithm is used. This algorithm generates key at registration stage and encrypts the ballot, vote. For generating key too large prime numbers which are kept secret, used as private key.

For privacy the contents of message are signed using blind signature, also a new key pair is generated using encryption and decryption phase[4]. RSA algorithm is chosen for this paper since factoring of large prime numbers is difficult. It was developed by for the purpose such digital signature, key exchange and encryption of small blocks of data. But its patent was expired on 2000.It uses two different keys namely public key and private key. Encryption of every message from sender to receiver requires public key which is known to all. Receiver requires private key to decrypt the cipher data. Both of the keys comprises of modulo 'n' and an exponent 'e' (for public key) and 'd' (for private key). This algorithm uses the method of exponentiation with squaring[5]. For encryption, (i.e.) plain text to cipher text, $c = m^e \bmod n_c$ and the conversion from cipher text to plain text (i.e.) decryption as plain text message, $m= c^d \bmod n$. the decryption process is faster than encryption. Encryption and decryption process of RSA is described in Figure-2.

Extended Euclidean Algorithm (EEA) is used by RSA to compute a unique number for private key. RSA generates key fast. But the decryption process is somewhat slower than the encryption process. Though it's a fast, the key generation is costly in terms of time consumption. RSA can be able to 'break' if given with sufficient resources and computational time. RSA is not suitable for smaller devices like mobile phone with less computational resources. It suffers by timing attack and consumes high power for computation.

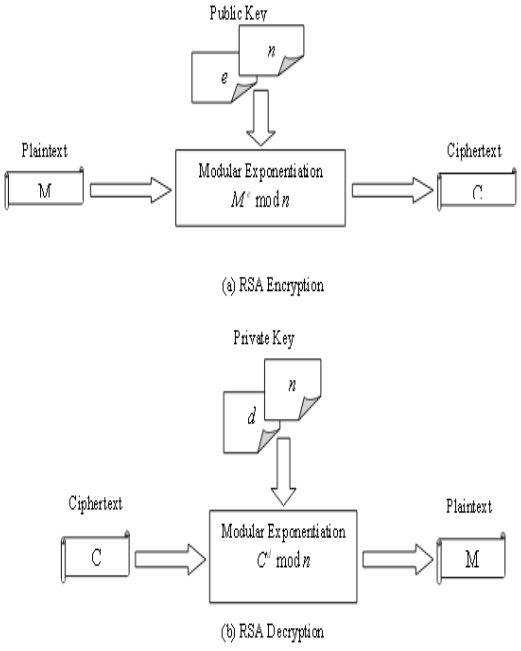

Figure 2. Encryption and Decryption of RSA.

5. Achieving Securities in Smart E- Voting System

Voting system consists of three layers. The first layer is the android application for votes to vote through mobile phone. The second layer comprises of a server provides the data demanded by voter. The third layer consists of a database that contains the details of voter. Here the system enables audit ability of votes. But vote secrecy, confidentiality and audit ability are the conflicting requirements[6]. The cryptographic algorithm used here is Elliptic Curve Cryptography (ECC) which was developed by Victor Miller (IBM) shown in Figure 3. It has less key size than any other algorithms. ECC is public-key cryptography based on ECDLP where the message is scrambled in elliptic curve (Figure-3). It can be easily explained by equation l.m = n, where l, n are the two points on curve. The hacker should find l, n to find the integer value 'm'. The elliptic curve can be describes by $Y^2=X^3+AX+B$, Where the variables X, Y are selected from finite field data set and A, B are the parameters of curve. Changing A, B will result in change of curve's shape. ECC combines number theory and algebraic geometry. The private key is computed and points to form curve are established. In terms of security, ECC of 160 modulo gives same cost as 1024 modulus of RSA and Elgamal. Though ECC, a strong algorithm, it consumes more time for key generation and encryption[7]. The fact is that the asymmetric algorithm consumes more time than symmetric algorithm for computation.

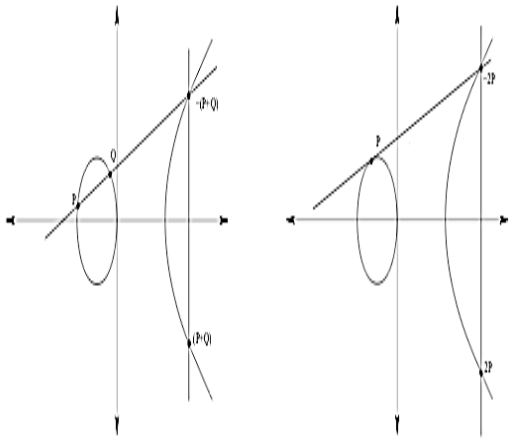

Figure 3. Elliptic Curve formation for plain text.

6. M-Vote: A Reliable and Highly Secure Mobile Voting System

This paper proposed an idea on mobile phone base voting which requires user id, password, and fingerprint for authentication and uses Advanced Encryption Standard (AES) as its cryptographic algorithm to encrypt and decrypt the user credentials and vote casted. AES is developed by Joan Daemon as an iterated block cipher. This paper described voting methodology with client-server communication system[8]. Here we use secret key since it is 1000 times faster than asymmetric key.AES is symmetric cryptographic algorithm which computes cipher text based on substitution and permutation which applies SKC schemes, known as Rijndael. As a successor of DES, AES was developed by NIST in the year 1997. The block size for AES is 128 bits. It uses various key that differ by length such as 128 bits, 192 bits and 256 bits to obtain cipher data. It produces high throughput with high speed. (Refer Figure-4 for AES encryption and decryption).

Though it's a strongest algorithm, the 44 mixed column process during encryption of plain text to cipher text and vice versa is costly in terms of time consumption. AES 128 bits need 10 cycles, 256 bits need 14 cycles, and 192 bits need 12 cycles. This may lead to poor throughput and more power consumption[9].

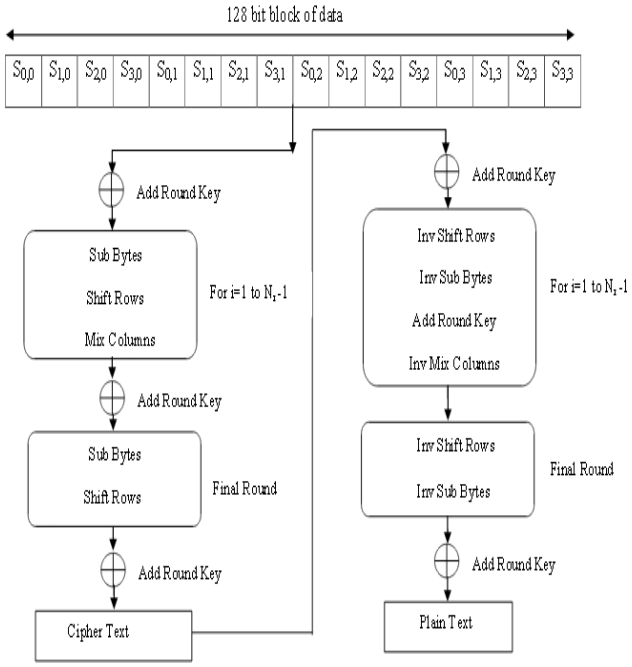

Figure 4. AES encryption and decryption.

7. BLOWFISH Algorithm

Figure 5 shows Feistal structure of blowfish Algorithm. It is a powerful secret key cryptography which accepts 64- bit plain text. Its key length ranges from 32 bits to 448 bits and has variable key length. It has minimum requirements for computation such as 32-bit processors, 5 kb memory size[10]. It is faster and secure than any other crypt-algorithms (refer Table 1).

This algorithm has 16 rounds consists of permutation, substitution and XOR (exclusive OR)[11]. The algorithm consists of two kinds of array namely s-array (4 s-boxes each with 256 entries) and p-array (p1 to p18). Unlike all algorithms, the encryption is not in reverse order of decryption, but the p-array entries are taken in a reverse order[12]. No successive crypt-analysis found for blowfish. The added advantage is that the algorithm is patent-free and can be used for general purpose[13]. The encryption and decryption process using this algorithm are faster. This algorithm is used by various application and e-commerce software which are practically implemented[14].

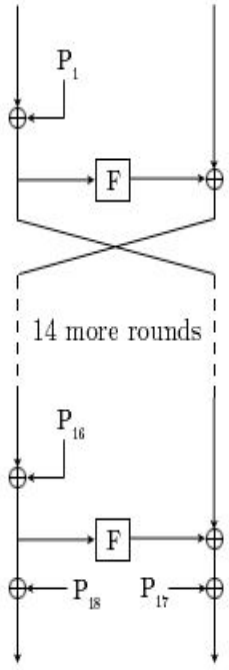

Figure 5. Feistel structure of blowfish algorithm.

Table 1. Comparison of file size and time taken for blowfish with other algorithms

Input size (KB)	Elgamal	RSA	AES	Blow fish
49	29	41	56	36
59	33	24	38	36
100	49	60	90	37
247	47	77	112	45
321	82	109	164	45
694	144	123	210	46
899	240	162	258	64
963	250	125	208	66
5345.28	1296	695	1237	122
7310.336	1695	756	1366	107
Avg. time	389	217	374	60.3
Throughput (MB/sec)	4.01	7.19	4.174	25.892

8. Conclusion

From the above result analysis, concluding that blowfish algorithm is superior in terms of efficiency, throughput, and speed less power and memory usage (refer Table 1, 2 and chart 2). The analysis on performance shows that blowfish is the best cryptographic algorithm than any other for the application such as voting which demands high security.

Table 2. Computational Time comparison for 256 MB data

Algorithm	Data	Time(sec)	Avg MB/ sec	Performance
Elgamal	128 MB	5	22-23	Low
RSA	128 MB	6	12	Low
AES	128 MB	2.5	51.2	Medium
Blowfish	128 MB	1.5-2	64	High

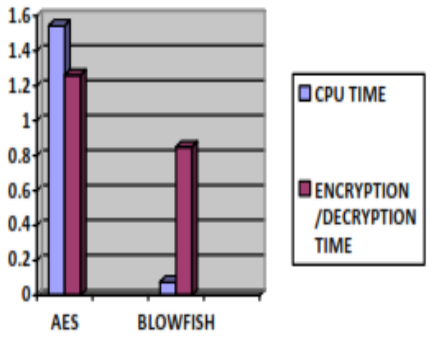

Chart 1. Comparison of AES and Blowfish.

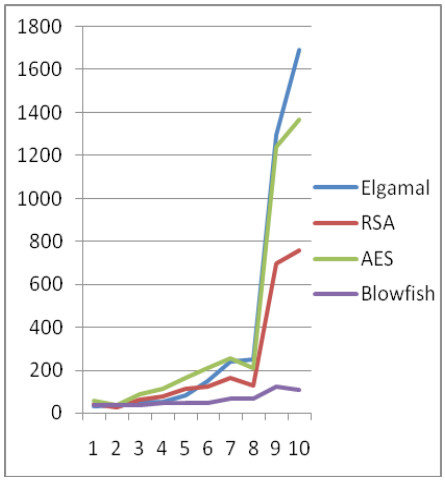

Chart 2. Time comparison based on input file size.

9. References

1. BhiseA, BorateN, GarjeA, Karkal Y. Secure Internet Voting System. The International Journal of Engineering and Science (IJES). 2015; 4(3):1–32.
2. Liu F, YanWQ. Visual cryptography for image processing and security theory, methods and applications: chapter-2: various problems in visual cryptography. 2014.
3. Brightwell I, Cucurull J, Galindo D, Guasch S. An Overview of the Ivote Voting System Spain. 2015; 1–25.
4. Thakur N, Ambavale V. E Voting Using Android System. International Journal of Science and Research (IJSR). 2015; 4(6):1–4.
5. Gura N, Patel A, Wander A, Eberle H, Shantz SC. Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs. International Association for Crypto Logic Research. 2004; 3156:119–32.
6. Kamble T, Jeyakumar A, Raut T. Achieving Securities In Smart E- Voting System. International Journal of Computer Engineering and Applications. 2014; 6(3):1–5.
7. Vivek B, Kute PR, Paradhi GR, Bamnote B. A Software Comparison of RSA and ECC. International Journal of Computer Science and Applications. 2009; 2(5):2–6.
8. Khelifi A, Grisi Y, Soufi D, Mohanad D, Shastry PVS. M-Vote: A Reliable and Highly Secure Mobile Voting System. Palestinian International Conference on Information and Communication Technology USA. 2013. p. 90–8.
9. Haldankar C, Kuwelkar S. Implementation of AES and Blowfish Algorithm. IJRET: International Journal of Research in Engineering and Technology. 2014; 3(3):1–4.
10. Kumar MA, Karthikeyan S. Investigating Efficiency of Blowfish and Rejindael (AES) Algorithms. I.J.C. N. I. S. 2012; 4(2):22–8.
11. Nagaraj S, Raju GSVP. Image Security using ECC Approach. Indian Journal of Science and Technology. 2015 Oct; 8(26):1–5.

12. Mahalakshmi U, Sriram VSS. An ECC based multibiometric system for enhancing security. Indian Journal of Science and Technology. 2013 Apr; 6(4):1–7.
13. Baek SS, Won YS, Han DK, Ryou JC. The Effect of Eight-Shuffling AES Implementations Techniques against Side Channel Analysis. Indian Journal of Science and Technology. 2015 Mar; 8(S5):1–7.
14. Vani PD, Rao KR. Measurement and monitoring of soil moisture using cloud IoT and android system. Indian Journal of Science and Technology. 2016 Aug; 9(31):1–8.