WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cybersecurity Awareness and Training with Advanced Cryptography Techniques

Md Salim[1] , Aishwarya Shekhar[2], Dr. Shambhu Kumar Singh[3]

[1]Department of Computer Science & Engineering, Sandip University, Madhubani, Bihar, India
[2,3]Department of Computer Science & Engineering, Sandip University, Madhubani, Bihar, India

ABSTRACT —

Cybersecurity Awareness in the organization & daily life is essential for human beings and any organization. In this paper, I will explain how data will be secure and safe for each individual and their privacy. I will also discuss how the new technologies are essential for security to avoid fraud and malpractices. Awareness can be considered in multiple ways to protect the privacies like "two-step verification for the authentication of the system, cipher text algorithm, RSA, DES & AES" Multiple advanced algorithms can be used by this to secure the system highly.

Simplifying complex concepts like breaking down topics, such as firewalls, encryption, or phishing into Layman's terms examples instead of talking about the complex cryptographic algorithms that "encryption is like locking our data safe" user-friendly training and communication that Create easy-to-digest materials like infographics, short videos, or interactive tutorials that guide non-technical users through best practices such as creating strong passwords, recognizing phishing attempts, or understanding the importance of software updates, sing gamified methods to engage users, such as through cybersecurity quizzes or simulated phishing attacks, to teach awareness in a fun and engaging way. These simplify the learning experience and give users immediate, actionable feedback.

Index Terms— RSA - Rivest – Shamir – Adleman, AES - Advanced Encryption Standard, DES - Data Encryption Standard , FY –Financial Year, RTI - Right to Information, Ad-Advertisement, Malware – Malicious Software, DDOS – Distributed Daniel of service attack, MIMT – Man-in-the-middle, XSS – Cross-site scripting, AI – Artificial Intelligence, NCRB – (National Crime Record Bureau), press Information Bureau.

INTRODUCTION

Today's world is suffering from multiple malpractices, cyberattacks, and cyber frauds. According to the data from the Reserve Bank of India, sent in response to the authors' RTI applications 0.003207 million was lost because of 0.582000 million cases of cyber fraud between FY 2020 and FY2024 published in "THE HINDU", newspaper on November 13, 2024. The above data particularly happened in India only in some specific year, think about the global how the people effects from the multiple cyber threat. There is a clear indication to implement the proper advanced infrastructure security, starting from the root level to higher authorities of the Government. This has made cybersecurity a necessary factor in the teaching of information systems with the development of malpractice groups such as Anonymous, whose sole purpose is to crack the information systems of different governments [1]. We know that millions of people don't know that how they can be reduced the multiple of cyber fraud. So, we be need to aware mass of the people who use different awareness techniques like Ad programs on social media e.g. Instagram, Facebook, and X, during dialing calls time on the phone. The government needs to make strategies to stop cyber fraud the society.

THEORETICAL FRAMEWORK

Multiple Methods of Cyberattacks.

There are multiple ways of attacking are possible nowadays with different strategies like Malware *(Viruses, Worms, Ransomware, Spyware, Adware),* Phishing *(Email, Spear, Whaling, Smishing, Vishing),* DDOS attacks, MIMT attacks, Password attacks *(Brute force attack, Dictionary attack, Keylogger),* SQL Injection Attacks, XSS attacks, Zero Day Attack, IoT Attacks are techniques that cyberattacks can be possible. Maximum attacks are performed through unsupervised use of the internet but the meaningful/information systems are attacked by different malicious software[1,2].

Challenges occurred during the cyberattacks.

Due to the cyberattacks/cyber frauds, we face multiple challenges for individuals, and businesses some major challenges include *financial losses* which mean malicious software like ransomware, phishing, and financial frauds result in significant monetary losses, and businesses may also face regular fines. Form *Data Breaches* Sensitive personal, financial, and business data can be stolen leading to identity theft intellectual property theft, or reputational

damage. *Operation disruptions* – attacks like DDOS can shut down websites, servers, and essential services disrupting operations and causing downtime. *National security threats* because of cyber warfare pose serious risks to national security, critical infrastructure, and defen*se. The psychological impact* that cyber harassment, cyberbullying, and social engineering attacks can cause stress, anxiety, and mental health for victims. *Intellectual property theft* – in this threat, hackers may steal trade secrets, patents, or research data which leads to financial and competitive disadvantages for organizations. *Emerging threats with AI and deepfake* that also cyber criminals use AI to create deepfake videos, conduct automated attacks, and enhance phishing techniques making cyber threats more sophisticated.

What do we know about the cryptography?

Cryptography is the practice and study of securing information through encoding techniques to present unauthorized access. It's the fundamental aspect of cybersecurity and is used in various applications such as secure communication, authentication & data integrity. Basically cryptography categories in *symmetric cryptography* (secret key), *asymmetric cryptography* (public key) & *Hash function.* In symmetric key cryptography which uses a single key for encryption and decryption of the data, firstly when we send the message package then encryption converts the plaintext to the cipher text by a single symmetric key again that this cipher text converts at the destination point into the plaintext by decryption techniques with similar key. So, in symmetric cryptography, we used the AES and DES technologies.

$[M_{\text{plain text}}] \rightarrow$encryption $\rightarrow$cipher text $\rightarrow$decryption $\rightarrow [M_{\text{plain text}}]$

Here M is considered as a Massage packet from sender to receiver,

Symmetric key cryptography simply converts the plain text to the coded information test that we know is cipher text with the help of the encryption key again received to the destination point then cipher text which is converted to the plain text with the help of the decryption key concept, in this key concept the secure the information by the cipher text techniques. Basically cipher text is in a coded format that is not readable by human beings so their data can be achieved the confidentiality, Symmetric key concept which is used the single key concept.

Note – Finding of the keys concept in symmetric cryptography which is defined as ${}^{n}C_{2}$ combination that is n is number of nodes.

Now let us talk about an asymmetric key concept which is also called public key cryptography, that each node has one private and one public key concept to encrypt and decrypt the proper messages. Like

[A] →----------→ [B]

Public A	Public B
Private A	Private B

In the above concept, we can find out the four cases like

Case 1: {public A[M]} -----encrypt----------[no one can open]
Case 2: {private B[M]} -----encrypt----------[no one can open]
Case 3: {private A[M]} -----encrypt----------[All can access, no confidentiality]
Case 4: {public B[M]} -------encrypt-------[accessible only required person with their personal private key].

There is high security provided that when we send a message publicly and the receiver accesses it own their private key that is mentioned in the case 4. In a symmetric key concept there is keys define 2N, here N is number of nodes given.

Cybersecurity awareness campaign in Asia and Europe.

There are various campaigns to improve the security for public security and business, we prescribe methodology cybersecurity awareness below: - *GetsafeOnline* [3] is popular in the UK and is initiated between several government bodies and multiple private sectors, their main purpose is to focus at home and in business too. The positive impact of the getsafeonline itself is an intriguing one, and it emphasizes to each individual that they have to be responsible for getting safe online activity. The campaign active malicious information if comes out and unwanted activity otherwise they change about being pre-alert of any sensitive information is very useful for the individuals. *The cyber streetwise campaign* [4] is used the boost cybersecurity and to reduce the multiple threats, so it works in mainly five ways: using strong memorable passwords like variations of keyword sections must be included, installing multiple antivirus software for each section of the device, strongly check the private section of the social application that do not give the access if you not used the such features, the security features and system before loading the cards details inside the system as soon as possible that they can be providing the more security. That's above two methods used frequently in the United Kingdom.

Cyber fraud and digital harassment in India

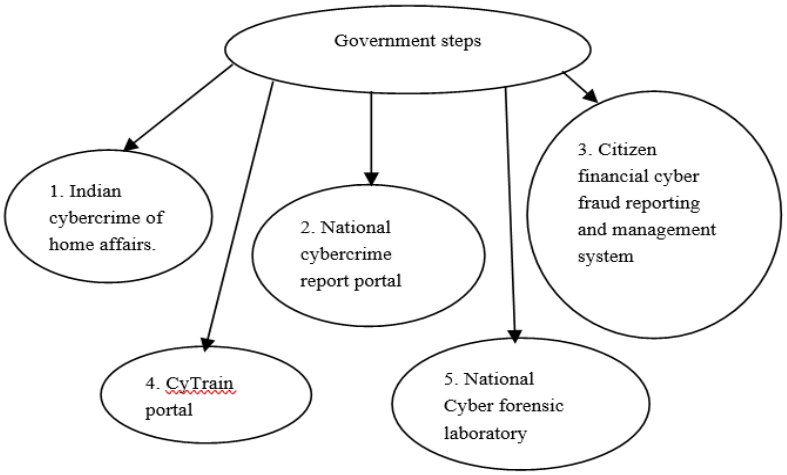
If we talk about India multiple fraud cases are happening nowadays that is their main agenda is earning financial profit from the use of multiple malpractices, the collection of individual data to be manipulated it's for multiple purposes like digital harassment. The NCRB analyzes and releases the statistics on crimes in cyber fraud, "published crime in India". Lastly publishing the report for the financial year 2022, the NCRB maintains information regarding certain categories of fraud for cybercrime like online payment systems, one-time password fraud, credit cards, ATM frauds, debit cards along many other problems. According to the report of NCRB, multiple fraud cases and fraud for cybercrimes that also involved communication devices were used as a medium for fraud that the report published in the year 2022. Their different crime report is mentioned below with a detailed analysis of fraud cybercrimes.

Number of cases	Transaction process	Transaction through	Fraud in the	OTP Related	Others	Total

under cybercrime	either debits or credits	ATM fraud	banking system through online	frauds		
	1665	1690	6491	2910	4714	17470

Source: Table 1 source from PIB Website Posted On: 03 DEC 2024 5:30 PM by PIB Delhi.

The data is too horrible for Indian society multilevel and multiple frauds are happening, day to day loop whole in the technologies to so we have to make it too much stronger along with Government of India having some strong and strength steps towards reduce the crime report and cyber fraud that related to the cyber security along with to ensuring the " privacy of data" of each individual to some steps taken by Government authorities are given bellows:-



1. If we take the Indian Government steps the Ministry of Home Affairs established the "Indian Cybercrime Coordination Center" under part of 14C. According to the Indian cybercrime coordination center to resolve and deal with all related issues of cyber fraud and cyber crimes. The main purpose to reduce and dealing the all reports related to cybersecurity and fraud too[3,4,5].

2. The government of India set the another entity that is "National Cyber Crime Reporting Portal", that is launched under section 14C by the Ministry of Home Affairs. Their main agenda is to report multiple cybercrimes, cyber fraud, child trafficking, women's harassment, and child abuse-related issues, especially for women and children. They can register FIR and other legal reports with the associated problems. The government's role in this portal that instantly transfer the report to the concerned states and union territories to take action as per the law established.
3. The government of India has also set the another bodies to control up the cybercrime happened financial related issued and that portal is launched in 2021 that is citizen financial cyber fraud reporting and management system under the regulation of 14 C.
   Their main purpose is to stop financial fraud happening in society, so citizen can free to register over there if they facing and fraud related cybercrimes. Authorities have more than rs. 3431crore (Indian rupees unit) from the 9.94 lakh(Indian rupees unit) complaints. They also launched the tall free number 130 to assist you any king of information and registered the complaints that related to the cybercrimes and cyber frauds.
4. The government of India developed the portal "CyTrain" under the section 14C, which gives the knowledge about the cybercrime investigation, prosecution happened with women & child and forensic used too.
   Total massive online open sources are available to grade up the knowledge about cybercrimes. In the CyTrain portal more then 98698 police officers are register for purpose to know aware about the multiple crime, easy to judgement etc. CyTrain platform issued more then 75591 certificates.
5. The last point is that the government of India set up a forensic laboratory at the Hyderabad (India), specially to collect the evidence and analyze the cybercrime report after compile it to easily detect the cybercrime related issues or work on the cybercrime related issued that is " National cyber forensic laboratory also help it to the government of India to boost the Indian Information Technology act.

Various cryptography techniques

Various types of cryptography techniques are given below:

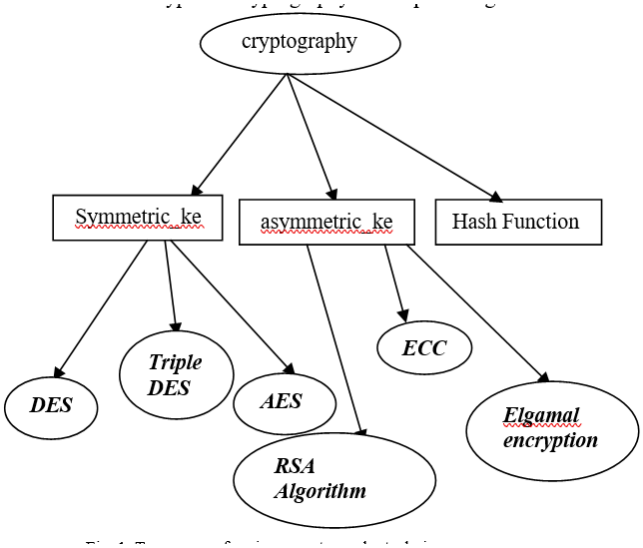


Fig. 1. Taxonomy of various cryptography techniques.

I already discussed the symmetric and asymmetric cryptography details in the theoretical methodology section. So now briefly explain the various techniques of cryptography given below:

- ***DES***

DES which is frequently used in symmetric key cryptography. It works on the principle of Feistel structure similar to block cipher. DES used 64 blocks where the key size is 56 blocks and the remaining 8 for parity. It's the most common cryptography attack so it is known as a plaintext attack, When have key size of DES is comparatively shorter than others a full search attacker can access the secret in DES cryptography, and also time attack is possible in this cryptography technique.

- ***AES***

AES is also a block cipher that replaces DES used for commercial applications with multiple variations. AES has a 128 bit block size with a key size defined 128,196 or 256 bits. AES is based on the swap permutation computing technique. Every sonorous uses four separate stages. Three are substitutions and one is permutation in this encryption standard. These three substitute mix columns, byte round key, and shift rows. AES is particularly used for compact devices[2].

- ***Triple DES***

The triple DES algorithm is a symmetric key block cipher that applies the DES algorithm three times to each block of data to enhance security. It becomes unsafe due to its short key length which is 56 bits. The triple DES algorithm encrypts data in three steps using either two or three keys that is encryption using the first key (Key 1), decryption using the second key (Key 2), and encryption again using the third key (Key3) this process is known as ESE process. Three key DES (Key1=Key3) that provide 168 bits key length (effective security ~ 112 bits). Two keys 3DES (Key1=Key3) that provide 112 bits key length (effective security ~80 bits). 3DES is used for better security than standard DES, still used in some financial and legal systems, although it's being phased out in favor of stronger algorithms like AES.

- ***RAS Algorithm***

The RSA algorithm is one of the bulk globally used public key cryptosystems. It's provided security even if an unsecure channel too[6,7].

Method of key generation in RSA algorithm.

- Take any two large prime numbers A and B.
- Now perform the product of the two prime numbers A and B that is A*B. now take N be the part of public key and private key both. Here security of RSA algorithm on the difference of factoring large numbers. So N is typically hundreds of digit long.
- After that calculate $\phi(x) = (A-1)*(B-1)$, where ϕ is Euler's totient function of the RSA algorithm.
- Again let the integer E, so that $1< E < \phi(N)$ where E is the module $\phi(N)$, this means $d*e = 1(\text{mod } \phi(N))$. Now the value of the public key is (E, N) and their private key is (d, N). again $Ct = M^e \text{ mod } N$, where Ct is the cipher text. Finally, we have to encrypt the cipher text Ct, the recipient uses their private key(d, N) where M is the original message[2,3].

- ***Diffie-Hellman key exchange***

The Diffie-Hillman key exchange is a method that allows the two parties to securely exchange the secret key wiith insecure channel, that means Diffie-Hillman key exchange provide the high security to the dat over a multiple parties It's one of the foundational ideas in public key cryptography. Public parameters mean everyone knows these.

Suppose a prime number is Pr which has its base Bg (that is also called the generator) which is less than the Pr. Now firstly find all aspects of Alice that suppose the private key is a1 and the key generated is $x1=(Bg)^{a1} \text{ mod } (Pr)$ again Bob has a private key that they select b1 and key generated $y1=(Bg)^{b1} \text{ mod } (Pr)$ here an exchange of generated key take place. Key received y1 by Alice and x1 keys by Bob again generated secret key by Alice $K_{a1}= (y1)^{a1} \text{ mod Pr}$ and Bob generated secret key $K_{b1}= (y1)^{b1} \text{ mod Pr}$. Finally, it shows that[3,5,6,7].

$$K_{a1} = K_{b1}$$

Therefore now have a symmetric secret key to encrypt. In practice, this is used with much larger numbers (hundreds or thousands of bits) to ensure security. It's often used in protocols like TLS/SSL (for HTTPS) and VPNs[4,7,8].

- ***Elliptic Curve Cryptography***

Elliptic Curve Cryptography is the public key cryptography that secures utilized data strongly with well-defined algebraic expression of an elliptic curve over a finite time field. It's more likely to be the RSA algorithm to provide data highly secure but the relatively key size is smaller along with the faster working process and also maintains the memory space utilized efficiently, The mathematical formula is: -

$$p^2 = q^3 + Aq + B$$

Where A and B are constants, and p and q are variables. The set of points (p, q) that satisfy this equation forms the elliptic curve.

Cipher_text	*Various keys type*	*Length of the keys in bits*	*List of attacks by symmetric and asymmetric key*
DES	*S.K. (symmetric key)*	*56*	*Chosen plaintext, Chosen ciphertext Brute force Attacks, Differential and Linear Cryptanalysis*
AES	*S.K. (symmetric key)*	*128,192 & 256*	*Related key attack, key recovery attack, Known plaintext, Side channel attack*
RSA	*A.K. (Asymmetric key)*	*1024 to 2048 (RSA is an asymmetric key so it depends upon N = A*B)*	*Factorization attacks, private exponent attacks, coppersmith's attack, Brute Force Attacks, Side Channel Attacks*
EL Gamal Encryption	*A.K. (Asymmetric key)*	*1024 to 2048*	*Fault attack, homomorphic property, Chosen Cipher text attacks.*
Elliptic Curves	*A.K (Asymmetric key)*	*160 to 256*	*Side channel attacks, fault injection attacks, Pollard's Rho method*

Table 2: Associative study of some widely used cryptosystems

Key size depends on the complexity of cryptographic algorithms. Again we compare the key size of two popular asymmetric cryptographic algorithms with one symmetric cryptographic algorithm according to the National Institute of Standards and Technology, so that is proved that ECC provides less complexity than the RSA algorithm.

ECC's relatively key size	*RSA relatively key size*	*Key Ratio*	*Overall AES key size*
163 bits	*1024 bits*	*(1 : 6)*	----
256 bits	*3072 bits*	*(1 : 12)*	*128bits*
384 bits	*7680 bits*	*(1 : 20)*	*192 bits*
512 bits	*15360 bits*	*(1 : 30)*	*256 bits*

Table 3: Comparative study of key size used in RSA and ECC

Over efficient cryptographic system implementation, the American National Standard Institute and National Institute of Standards and Technology are producing standards and technology about that related topic[1,2,5].

CONCLUSION

In this paper, we work on the multiple dimensions of cyber security awareness like how to implement lawfulness by the legal authorities into the mass impact into the society. We know about the different technologies that the different key concepts in this thesis paper, also giving the awareness program with the help of different organizations like the Indian government's current policy for awareness, after that we implement multidimensional security into the different protection techniques like talking about the symmetric key concept technologies (AES, DES, 3DES) and asymmetric key concept technologies like that the RSA algorithm, EL Gamal encryption ad elliptic curves. Where the bit length of every cipher text has different likewise 56 bits (DES), 128its,196 bits, and 256 bits(AES), RSA (1024 – 2028bits) based on the number of bits in N=P*Q and E L Gamal encryption that exists 1024 -2048 bits. So basically try to focus on the awareness society of cyber threats and how to prevent data from malicious practices by using advanced cryptography techniques.

ACKNOWLEDGEMENT

In this paper "Cybersecurity Awareness and Training with advanced cryptography techniques", I used the British Langua technique. Also taking the resources from multiple newspapers like Indian Express, The Hindu, etc.

REFERENCES

[1] Bibhu Dash, Meraj F. Ansari, "An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy," vol. 9,4 April 2022, e-ISSN: 2395-0056, p-ISSN: 2395-0072.

[2] W.-K. Chen, *Lin22ear Networks and Systems* (Book style). BelT. Siegenthaler, Decrypting a class of stream ciphers using ciphertext only, IEEE Trans. Comput.,34, 81-85, 1985. mont, CA: Wadsworth, 1993, pp. 123–135.

[3] GetSafeOnline Campaign [Accessed online November 2014] www.getsafeonline.org

[4] The Cyber Streetwise campaign [Accessed online November 2014] www.cyberstreetwise.com

[5] GetSafeOnline Campaign [Accessed online November 2014] www.getsafeonline.org

[6] Christof Paar and Jan Pelzl, Understanding Cryptography, Springer, 2010

[7] T. Siegenthaler, Decrypting a class of stream ciphers using ciphertext only, IEEE Trans. Comput.,34, 81-85, 1985.

[8] Jitendra Singh Chauhan and S. K. Sharma, "A Comparative Study of Cryptographic Algorithms," Int. J. Innov. Res., pp. 24–28, 2015.

[9] A. Al Hasib and A. A. M. M. Haque, "A comparative study of the performance and security issues of AES and RSA cryptography," Proc. - 3rd Int. Conf. Converg. Hybrid Inf. Technol. ICCIT 2008, vol. 2, no. November 2001, pp. 505–510, 2008.

[10] C. Narasimham and J. Pradhan, "Evaluation of Performance Characteristics of Cryptosystem Using Text Files.," J. Theor. Appl. Inf. Technol., vol. 4, no. 1, 2008.

[11] M. Mikhail, Y. Abouelseoud, and G. Elkobrosy, "Extension and Application of El-Gamal Encryption Scheme," 2014.

[12] A. Naureen, A. Akram, T. Maqsood, R. Riaz, K. H. Kim, and H. F. Ahmed, "Performance and security assessment of a PKC based key management scheme for hierarchical sensor networks," IEEE Veh. Technol. Conf., pp. 163–167, 2008.

[13] M. Albrecht, and C. Cid. Algebraic Techniques in Differential Cryptanalysis. Proceedings of the First International Conference on Symbolic Computation and Cryptography, SCC 2008, Beijing, China, April 2008.

[14]] E. Biham, and A. Shamir. Differential Cryptanalysis of the Full 16-round DES. Advances in Cryptology – CRYPTO 1992, Lecture Notes in Computer Science, vol. 740, Springer–Verlag, pp. 487–496, 1992.

[15] M. Matsui, "On the correlation between the order of S-boxes and the strength of DES", Advances in Cryptology, Proceedings Eurocrypt'94, LNCS 950, A. De Santis, Ed., Springer-Verlag, 1995, pp. 366-375.

[16] V. Rijmen, B. Preneel, "A family of trapdoor ciphers", Fast Software Encryption, LNCS 1267, E. Biham ed., Springer-Verlag, 1997, pp. 139-148.

[17] KELIHER, L.: Refined analysis of bounds related to linear and differential and linear cryptanalysis for the AES, in: Advanced Encryption Standard—AES '04, 4th Internat. Conf. (H. Dobbertin et al., eds.), Bonn, Germany, 2004, Lecture Notes in Comput. Sci., Vol. 3373, Springer-Verlag, Berlin, 2005, pp. 42–57.

[18] DAEMEN, J.—RIJMEN, V.: The Design of Rijndael: AES—The Advanced Encryption Standard. Springer-Verlag, Berlin, 2002.

[19]] G. N. Nayak and S. G. Samaddar, Different flavors of man-in-the-middle attack, consequences and feasible solutions, Chengdu, 3rd IEEE International Conference Volume 5, pp 491-495, 2010

[20] B. Isaac, Secure ARP and Secure DHCP Protocols toMitigate SecurityAttacks. Int. Journal of Network Security 8: 107-118, 2009

[21] Jana Bappaditya, Poray Jayanta (2016) A performance analysis on elliptic curve cryptography in network security, 10.1109/ICCECE.2016.8009587, ISBN: 978-1-5090-4432-0

[22] Improving Divide and Conquer Attacks against Cryptosystems by Better Error Detection / Correction Strategies Werner Schindler, Franc¸ois Koeune, and Jean-Jacques Quisquater B. Honary (Ed.): Cryptography and Coding 2001, LNCS 2260, pp. 245–267, 2001. c Springer-Verlag Berlin Heidelberg 2001

[23] P. Nalwaya, V. P. Saxena, and P. Nalwaya, "A cryptographic approach based on integrating running key in feedback mode of elgamal system," Proc. - 2014 6th Int. Conf. Comput. Intell. Commun. Networks, CICN 2014, pp. 719–724, 2014.