International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.327-336
http://dx.doi.org/10.14257/ijsia.2016.10.5.31

Coherent Caesar Cipher for Resource Constrained Devices

Priya Verma[1], Gurjot Singh Gaba[2]

[1,2]Discipline of Electronics and Communication Engineering,
Lovely Professional University,
Phagwara, Punjab, India - 144411
priyaverma1740@gmail.com[1], er.gurjotgaba@gmail.com[2]*
([2]Corresponding author[*])

Abstract

Today, cryptography is a cornerstone in the resource constrained networks and devices. Many modern cryptosystems make it very difficult but not impossible for an attacker to determine the decoding key. Even though the key might be eventually determined by a skilled decoder, given enough time and effort, cryptosystems can still provides ample security to protect valuable information. Among various encryption techniques, Caesar cipher is one of the oldest technique to encrypt the valuable information. But it gets easily cracked due to its simplicity of operation. In this paper, a new algorithm is proposed i.e. Coherent Caesar Cipher (CCC), which is found to be more consistent and reliable as compared to other existing caesar cipher algorithms. Performance of CCC and conventional techniques are tested using various NIST suggested randomness evaluation tests along with brute force attack analysis. The results were promising as the proposed technique produced more random results for various inputs and has the capability to withstand brute force attack for a longer duration.

Keywords:*Cryptography; Caesar cipher; Encryption; Security; Brute force attack.*

1. Introduction

Cryptography is invented for safely transmission of knowledge, within the existence of any adversaries. In cryptography, encryption is done at the transmitter end so that no attacker will get access of data while it is on the way. To prevent disclosure of data to unauthorized parties, many cryptography encryption techniques were evolved in the past [1]. One of the design parameters of Encryption technique is to ensure that the cost of carrying an attack exceeds the cost of plaintext. It is possible with enlargement of key size which would provide resistance against attacks. For the short length keys, it is easy for an attacker to attack on the plaintext by trying all the feasible combinations of the key. If the size of the encoding key is larger, it would be difficult for an attacker to determine the plaintext, as it takes hundreds or thousands of years to decrypt. Another objective of Information Security systems is to guard data resources at a price less than the worth of the data that's being protected. In cryptosystems, the plaintext is encrypted with encryption algorithm and the secret key; which generates a coded message called as ciphertext. The entity that is having the secret key can only be able to decrypt the message. The Key size should be large enough and must be shared in a secure way with the recipient so that even if someone figures out the attributes of decoding key, still it would be difficult for them to convert the ciphertext into plaintext [2]. There may also be chances of forgery by the attacker if the ciphertext and decoding key is known [3]. Therefore, cryptography systems must provide the confidentiality, source authentication and integrity. If any third party knows the way to access the coded messages, still they won't be able to decrypt it, because only the authorized recipient has the key sent by the

ISSN: 1738-9976 IJSIA

sender required for decryption. Cryptography should develop mechanisms and different techniques which ensures the authenticity of the recipient and sender to overcome the forgery problems. So, diverse encryption techniques subsist in cryptography are: Caesar cipher, Playfair cipher, One time pad cipher etc [4]. One of the most primitive technique is Caesar cipher which is more vulnerable to brute force attack. An elongate approach of Caesar cipher is proposed in this paper which yields more security than the conventional Caesar encryption techniques.

2. Related Work

L. Han et al. (2014) in paper entitled "*An Implementation of Caesar Cipher and XOR Encryption Technique in a Secure Wireless Communication*" proposed a way for the secure transmission of knowledge over the networks, that concerns three phases i.e. secret writing encryption technique, serial port communication program and cryptography pattern style. The encryption technique utilized in this paper is Caesar cipher. Caesar cipher is made complex by merging existing Caesar cipher technique with XOR secret writing. The XOR secret writing uses bitwise XOR operations to get the specified quality and randomness in Ciphertext. A comparison on the premise of data co-ordinated time has been done to prove the potency of advised technique over the prevailing ones. The blending of Caesar cipher and XOR secret writing has not affected the interval of data and has proved to provide a secure wireless communications [6].

A. Rajan et al. (2014) in paper entitled "*Advancement in Caesar cipher by randomization and delta formation*" proposed a new technique to modify the Caesar cipher. In this, encryption method is divided into three stages which involve Randomization, Encryption and delta formation. The proposed technique yields potential combinations 26!9! of ciphertext which makes very difficult for an offender to determine the original plaintext[7].

G. Patidar et al. (2013) in paper entitled **"***A block based encryption model to improve avalanche effect for data security"* states that for the security of data a block based cryptography model is introduced which employs a combination of computing and logical function. The authors compared the various encryption techniques like Caesar cipher, Vigenere cipher, Playfair cipher, DES and AES on the basis of their memory utilization, CPU utilization, throughput and avalanche effect. From the results it is analyzed that caesar cipher, vigenere cipher, playfair cipher has very less Avalanche effect i.e. 2%, 4% and 8% respectively, whereas CPU and Memory usage is 1.56%, 3.13% and 6.25% respectively. It is found from the review that though modern encryption schemes such as DES and AES consume more power (54.68% and 66.23%) still they are better because of high avalanche effect (60% and 70%) [9].

D.K. Gupta et al. (2012) in paper entitled, "*New Concept of symmetric encryption algorithm a hybrid approach of caesar cipher and columnar transposition in multistage"* states that traditional Caesar cipher is changed by interbreeding it with columnar transposition to create the new, safer and robust technique. During the implementation, they have used two totally different keys for the Caesar cipher (substitution algorithmic program) and columnar transposition (transposition algorithmic program). Here transformation is done on the encrypted message which is received from the Caesar cipher code. The key for the Caesar cipher plays a major role in columnar transposition secret writing. This algorithmic program uses two secret writing keys which may pose difficulty to perform brute force analysis. Results indicate that assailant now requires long-time to decipher the message [10].

3. Proposed Technique (CCC)

Caesar cipher gets easily affected by an attacker because it has only 26 keys to encrypt the message. So brute force attacker can easily try all the possible combinations of keys and decode the ciphertext. Hence, information is less secure in Caesar cipher. To overwhelm the shortcomings of previously existing Caesar ciphers, a new approach is proposed in this paper which is named as *Coherent Caesar Cipher (CCC)*.

Operation of proposed technique is divided into four parts:-

a) Substitution in plaintext

b) Secret key generation

c) Encryption procedure

d) Decryption procedure

3.1 Substitution in Plaintext

The plaintext can be made secure before the starting of encryption process. In our proposed technique plaintext characters are initially replaced by characters of alphabets in the decreasing order**.**

Sequence of characters in increasing order	a b c d e f g h i j k l mn o p q r s t u v w x y z
Sequence of characters in decreasing order	z y x w v u t s rq p o n ml k j i h g f e d c b a

Let us take the plaintext input as "processing". According to the algorithm, the plaintext characters are replaced with the sequence of characters in decreasing order.

Plaintext	processing
Substituted plaintext result	kilxvhhrmt

3.2 Secret Key Generation

Key plays a very crucial part during the encryption process. Key generation function must be complex and robust while reciprocating the information over the network. In this proposed technique secret key generation process is splitted in three parts which depends on the key value.

Key ranges:

(i) **Key 1<=3:-** If key value lies in the range 1<=3, then it evaluates the factorial followed by compliment of it and then transform the key into its binary form. In the latter section, four complimented bits are prepended to the four bit factorial output, thereby forming 8 bit key.

(ii) **Key 3<=15:-** If key value lies in the range 3<=15, then converts the key value directly into its binary equivalent followed by bits compliment. Afterwards these four complimented bits are prepended to the four bits of binary equivalent output.

(iii)**Key 15<=255:-** If key value lies in the range 15<=255, convert the key value straightly into its binary equivalent.

Suppose the key value as 3, then the final key obtained as per the rules of proposed technique would be 10010110.

Key value	3
Factorial	6 (0110)
Bit compliment	9 (1001)
Binary equivalent of key	10010110

3.3 Encryption Procedure

To make the data not easily understood by an unauthorized person, encryption technique is used**.** The information is protected in such a way so that only an authorized user can read it. Let us take the first substituted plaintext character of input “processing” i.e. ‘k’. By performing the XOR of the first 4 bits of the substituted plaintext character ‘k’ with the last four bits of the key value and the last four bits of the substituted plaintext character with the first four bits of key value, we get partial cipher text result C_1 followed by NOT operation resulting in C_2.

Plaintext	‘processing’
Substituted plaintext result	‘kilxvhhrmt’
ASCII Binary equivalent of ‘k’	01101011
Key value	10010110
Partial ciphertext (C_1)	00000010
‘NOT’ operation (C_2)	11111101
Final ciphertext (C_3)	11111101

Aftermost, reorganize the bits of C_2 corresponding to the following pattern mentioned in the table 1.

Table 1. Schedule of Reorganizing the Bits

Bit Location	1	2	3	4	5	6	7	8
Shuffle Pattern	1	8	6	2	3	4	7	5

Final ciphertext attained after reorganizing (C_3) = 11111101.

The final ciphertext in character form can be recovered by calculating the decimal value of C_3 which comes out to be ‘253’ and then finding the corresponding ASCII character value, in this case it is ‘ý’. So ‘p’ is encrypted as ‘ý’. Similar process is carried out to encrypt the other remaining characters of input ‘processing’.

The encrypted result for ‘processing’ is ‘**ýÿ»¿¿¸ß**

3.4 Decryption Process

The original plaintext information can be recovered easily if the whole process is reversed.

4. Results and discussion

Different tests are carried out on all the techniques using same inputs to examine the potency of the proposed technique.

4.1 Avalanche Effect

One of the important considerations for measuring the strength of any cryptographic algorithm is its Avalanche Effect. A good algorithm should produce high Avalanche Effect. It is defined as the number of flipped bits in the ciphertext to the total number of bits in the ciphertext [8].Table 2 indicates the percentage of avalanche effect for all the techniques corresponding to different values of inputs

$$Avalanche\ effect = \frac{No.of\ flipped\ bits\ in\ the\ ciphertext}{Total\ no.of\ bits\ in\ the\ ciphertext} * 100 \tag{1}$$

Table 2. Avalanche Effect Analysis

Encryption techniques	**Key**	**%age of bits flipped for different keywords**				
		Old	*site*	*Search*	*picture*	*processing*
Basic Caesar (B.C) [21]	3	33.33	28.12	29.16	30.35	35
XOR technique [10]	3	33.33	25	25	25	23.75
Delta formation [22]	3	NA	NA	NA	NA	NA
Coherent Caesar Cipher (CCC)	3	**66.66**	**68.75**	**58.33**	**60.71**	**62.50**

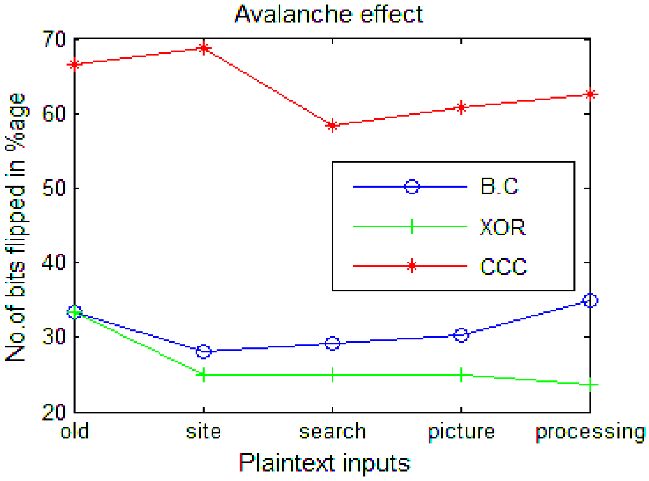

Figure 1. Comparison of Different Algorithms based on Avalanche Effects

Fig.1 shows the performance of encryption techniques in terms of avalanche effect. Here, we compare the avalanche effect of basic Caesar, Caesar using XOR technique and coherent Caesar cipher technique over different plaintext inputs. Our results show that proposed technique (CCC) has more no. of flipped bits than other existing algorithms therefore resulting in high avalanche effect. Due to the dissimilar length of plaintext and ciphertext in delta formation technique, avalanche effect is not predictable. It also consumes more processing power and memory.

4.2 Frequency Test

The focus of this test is to find the proportion of zeros and ones for the entire sequence. The purpose of this test is to determine whether the number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence. The test assesses the closeness of the fraction of ones to 1/2, that is, the proportion of ones and zeros in a sequence should be about the same [8]. Firstly the zeroes and ones of the input sequence is converted to values of -1 and +1 and added together to produce S_n, then Compute the test statistic (*sobs)* and p-value. If the p-value is > than 0.01, then conclude that sequence is random otherwise it is non random.

Where $$sobs = \frac{|Sn|}{\sqrt{n}} \qquad (2)$$

$$P_{value} = erfc\frac{sobs}{\sqrt{2}} \qquad (3)$$

Table 3. Frequency Test Analysis

Encryption techniques	***Key***	***Frequency of 0's and 1's for different keywords (%age)***				
		Old	*site*	*Search*	*picture*	*processing*
Basic Caesar [21]	3	0.6250	0.5625	0.5208	0.5536	0.5375
XOR technique [10]	3	0.4583	0.5313	0.4375	0.5714	0.5750
Delta formation [22]	3	0.5048	0.5673	0.5481	0.5529	0.5096
Coherent Caesar Cipher (CCC)	3	**0.6667**	**0.5938**	**0.7083**	**0.6607**	**0.7375**

Table 3 shows the percentage of 0's and 1's for multiple inputs to test the randomness of the ciphertext result for all the techniques.

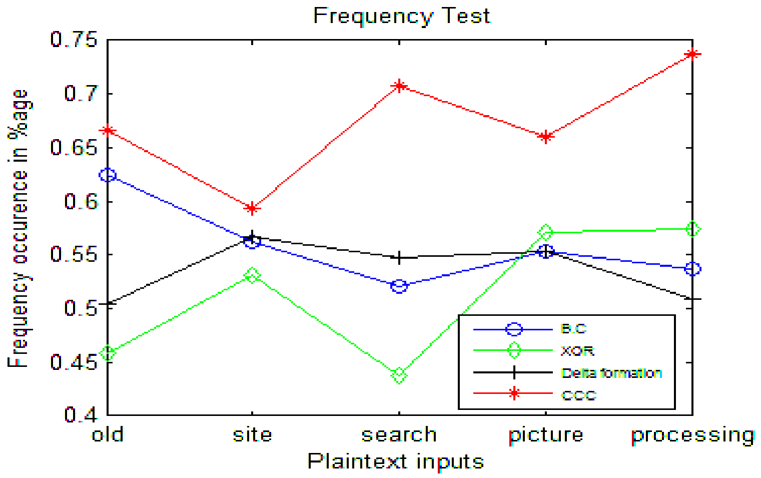

Figure 2. Comparison of Different Algorithms based on Frequency Test

Fig. 2 depicts the performance of different algorithms on the basis of frequency test. Our results clarifies that proposed technique (CCC) presents significant results as compared to the other algorithms. The probability of equal number of 0's and 1's is high in Coherent Caesar Cipher (CCC) technique. This means that sequence produced by CCC is more random and can't be easily cracked by an adversary.

4.3 Binary Derivative Test

The binary derivative test is useful to measure the randomness of a binary string.. For a sequence to be random, the output value should lie near to 0.5. The first binary derivative of S_1, $D_1(S_1)$, is the binary string of length n - 1 formed by XORing adjacent pairs of digits[8].If the value of P_{avg} is near to 0.5 than the sequence is random otherwise it is non random.

$$P_{avg} = \frac{S_1}{n} \tag{4}$$

Table 4 points out the various output values obtained by giving different inputs to various techniques.

Table 4. Binary Derivative Test Analysis

Encryption techniques	***Key***	***Binary Derivative test for different keywords (%age)***				
		old	*site*	*Search*	*picture*	*processing*
Basic Caesar [21]	*3*	0.5440	0.5625	0.4783	0.4752	0.4799
XOR technique [10]	*3*	0.4880	0.5361	0.4428	0.4586	0.4748
Delta formation [22]	*3*	0.4461	0.4661	0.4628	0.4489	0.4636
Coherent Caesar Cipher (CCC)	*3*	**0.5040**	**0.5176**	**0.4848**	**0.4890**	**0.4810**

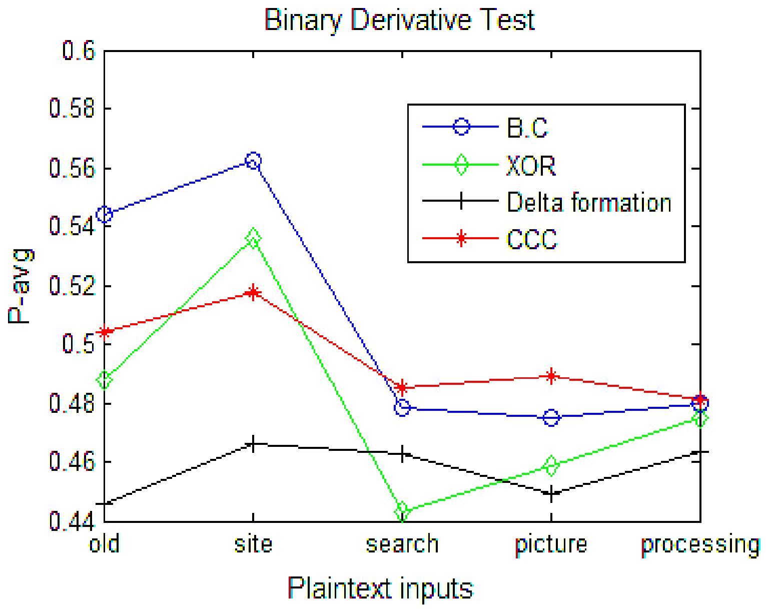

Figure 3. Comparison of Different Algorithms based on Binary Derivative Test

Fig.3 is graphically creating distinction among various techniques on the basis of binary derivative test. For all the multiple inputs, proposed technique (CCC) has produced output value that lies near to 0.5 which indicates more randomness in the sequence. Rest all the existing algorithms has the values far away from 0.5 which shows non randomness.

4.4 Resistance to Brute Force Attack

In brute force attack, all possible set of combinations is applied by the attacker on cipher text until to recover the plaintext. Traditional Caesar cipher is the most affected due to less no. of keys. Brute force attacks are carried out by applying all possible keys uniformly until the plaintext is recovered. Brute force attack effect is reduced by complicating the information and make it in such a way that attacker cannot identify it when the code is cracked. To find the strength of encryption system is how long it would taken by the attacker theoretically to apply a brute force attack successfully on it. From table 5, we can analyze that proposed technique (CCC) has advantage over the existing Caesar cipher techniques, as the brute force attack is difficult to carry in CCC than existing techniques. From table 5, it is observed that the time required for decrypting the word ‘processing’ in Basic Caesar cipher requires 558.015sec, XOR technique requires 1468.2404sec whereas proposed technique (CCC) requires 15804.435sec. Hence, more time is required for an intruder to deciphering the message in proposed technique (CCC), thereby putting stronger and securable impact on encryption result. Figure 4 depicts that our proposed technique (CCC) is highly securable as it requires 4.39 hours / 263.4 minutes / 15804.435sec to decrypt the message. This technique can be incorporated in the process of encryption of any plaintext. Hence this technique is unconditionally secure.

Table 5. Brute Force Attack Analysis

Plain text (Input)	**KEY SIZE**	**Basic Ceaser Cipher [5]**		**XOR technique [6]**		**Delta formation [7]**	**CCC (Proposed)**	
		Cipher text	***Brute force attack time (sec)***	***Cipher text***	***Brute force attack time (sec)***	***Brute force attack time (sec)***	***Cipher text***	***Brute force attack time (sec)***
old	3	rog	153×10^{-9}	lpi	183×10^{-9}	NA	ÝØ	371×10^{-9}
site	3	vlwh	275×10^{-8}	pkyi	471×10^{-8}	NA	¿¸Ü	122×10^{-7}
search	3	vhdufk	319×10^{-5}	pgdtdp	321×10^{-5}	NA	¿¹ÿ»ø	133×10^{-4}
picture	3	slfwxuh	432×10^{-4}	skbzzvl	835×10^{-4}	NA	ý¸»Üÿ	44×10^{-2}
Proces-sing	3	surfhvvlqj	558.015	Srncju-vqum	1468.2404	NA	ýÿ»¿¿¸ß	15804.435

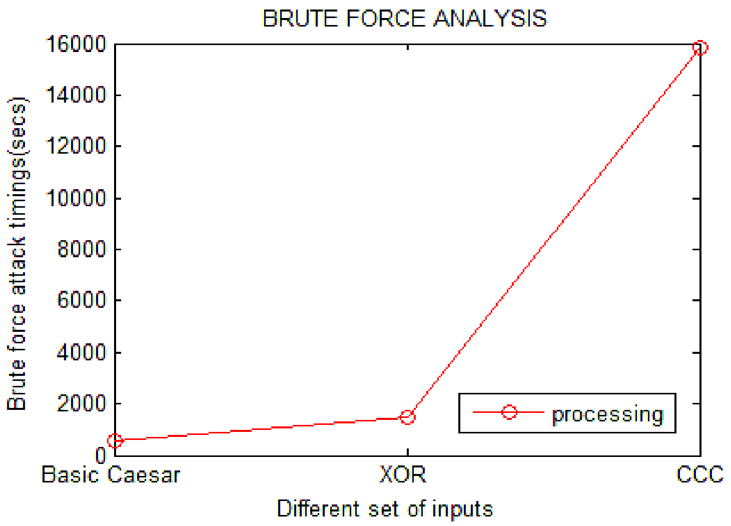

Figure 4. Comparison of Different Algorithms based on Brute Force Analysis

5. Conclusion

Caesar Cipher encryption technique is considered to be less secure as it uses only 26 possible set of keys for encryption. To enhance its strength, a new technique is suggested in this paper named as Coherent Caesar Cipher (CCC).The proposed technique has passed various tests recommended by NIST i.e. avalanche effect, frequency test, binary derivative test. Moreover, brute force attack is carried on the encrypted results of all the algorithms, which proved that proposed technique (CCC) can withstand the brute force attack for a longer duration.

References

[1] R. Mane, "A Review on Cryptography Algorithms, Attacks and Encryption Tools," International Journal of Innovative Research in Computer and Communication Engineering., vol. 3, no. 9,**(2015),** pp. 8509-8514.

[2] S. Kaushik and A. Singhal, "Network Security Using Cryptographic Techniques," International Journal of Advanced Research in Computer Science and Software Engineering., vol. 2, (**2012**), pp.105-107.

[3] S. Chandra, "A comparative survey of Symmetric and Asymmetric Key Cryptography," International conference on Electronics, Communication and Computational Engineering (ICECCE), Hosur, (**2014),** pp. 83–93.

[4] S. Shakti, "Encryption using different techniques," International Journal in Multidisciplinary and Academic Research (SSIJMAR)., vol. 2, no. 1, (**2013**), pp. 1-9.

[5] O. Abraham and Ganiyu O. Shefiu, "An improved Caesar cipher algorithm," International Journal of engineering science and advanced technology., vol. 2, (**2012**), pp.1199-1202.

[6] L.C. Han, N.M. Mahyuddin, "An Implementation of Caesar Cipher and XOR Encryption Technique in a Secure Wireless Communication," 2nd International conference on Electronic Design (ICED), Penang, **(2014),** pp.111-116.

[7] A. Rajan and D. Balakumaran, "Advancement in Caesar cipher by randomization and delta formation," International conference on Information communication and Embedded systems (ICICES), Chennai, (**2014)** pp.1-4.

[8] William Stallings, "Cryptography and Network Security: Principles & Practices", New York, NY: Pearson Education, (**2006).**

[9] G. Patidar, N. Agrawal and S. Tarmakar, "A block based encryption model to improve Avalanche Effect for data security", International Journal of Scientific and Research Publications., vol. 3, **(2013),** pp.1-4.

[10] D. K Gupta, S. Ksrivastava, and V. Singh, "New concept of symmetric encryption algorithm a hybrid approach of Caesar cipher and columnar transposition multi stages", Journal of Global Research in Computer Science ,vol. 3, no. 1,(**2012**), pp. 60-66.

Authors

Gurjot Singh Gaba, is currently pursuing Ph. D. in Electronics & Electrical Engineering with Spl. in *Cryptography and Network Security of WSN and IoT's*. He is working as an Asst. Prof. in Lovely Professional University since 2011. His research interest includes Wireless Sensor Networks, Computer Networks, Optical Communications and Cryptography. He is currently engaged in the project of 'Micro Satellite'. He is an author of six International books and more than two dozen research papers.

Priya Verma, is currently pursuing M.TECH in Electronics and Communication Engineering with Spl. in Wireless Communication Systems at Lovely Professional University, India. Her research interests include Wireless Sensor Networks and Cryptography.