INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 3)
Available online at: www.ijariit.com

Cryptography techniques: A survey

Pooja Kallolimath
poojakallolimath@gmail.com
K. L. S Gogte Institute of Technology, Belgaum, Karnataka

Dr. Prashant P. Patavardhan
pppatavardhan@git.edu
K. L. S Gogte Institute of Technology, Belgaum, Karnataka

ABSTRACT

In recent years network security has become a very important issue. Encryption has come up as a solution, and plays an important role in data security system. Several techniques are required to protect the shared data. Most commonly used encryption algorithms in the domain of cryptography firstly to identify their weaknesses and vulnerabilities and secondly to identify the aspects of those weaknesses which will be avoided by correct implementation. In this paper, we provided different types of encryption algorithms that are existing and literature survey of those algorithms.

Keywords: *Network security, Cryptography, Encryption, Decryption, DES, 3DES, AES, RC5, BLOWFISH, RSA.*

1. INTRODUCTION

Use of the Internet is growing rapidly. So, providing security to the information over networks has become a crucial issue these days. Information over networks is insecure, it should be disclosed solely to the meant recipients, not to everybody. Information is more prone to attacks while transmitting in the network. Cryptography provides security to information and solutions to all the problems of network security. It makes the messages immune to different attacks by converting the original message into the coded message. Encryption is used for converting the original message into the disguised message at the sender end. Various cryptography algorithms are used to hide the content of the message from all except the sender and the receiver.

1.1 Basic concepts of Cryptography

- Plain text: Plain text is the original message which is to be encrypted at the sender end.
- Cipher text: Cipher text is the coded message which is to be decrypted at the receiving end.
- Intruders: Intruders alter the message with wrong intentions. Intruders fabricate the original messages and send their own disguised messages.
- Encryption: Encryption is a process that converts Plain text into Cipher text [7]. It requires Encryption algorithm and a key.
- Decryption: decryption is a process that converts Cipher text into plain text. It requires Decryption algorithm and a key.
- Key: Key operates on the plain text and converts it into cipher text. It is used for both Encryption and Decryption Processes. Key could be a number, function or an algorithm [1].

1.2 Classification of Cryptography

- Symmetric Key Cryptography: In Symmetric key cryptography [1] the key used for encryption is similar to the key used in decryption. Therefore the key distribution has to be made prior to the transmission of information. The key plays a very important role in symmetric cryptography since their security depends on the nature of key i.e. the key length etc [4]. There are various symmetric key algorithms as shown in Figure 1.
- Asymmetric Key Cryptography: Asymmetric key cryptography is also known as Public key cryptography which uses two different keys for encryption and decryption [1]. The keys are large numbers that have been paired together but are not identical. One key will be shared with everyone, it is referred as the public key. The other key in the pair is kept secret, it is referred as the private key. Either of the keys can be used to encrypt or decrypt a message [10]. Most popular asymmetric key algorithm is RSA algorithm.

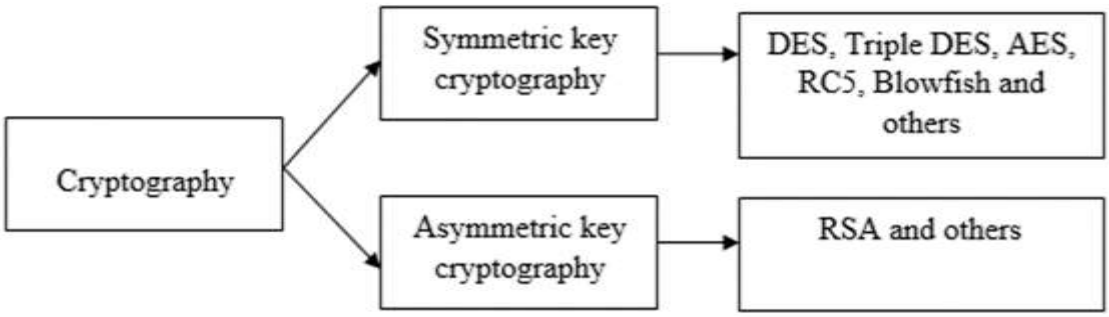

Figure 1: Classification of Cryptography

2. LITERATURE SURVEY AND OVERVIEW OF ALGORITHMS

In cryptography variety of conventional encryption algorithms are available. Some of the symmetrical algorithms are DES, Triple DES, AES, Blowfish, RC5, etc. and asymmetrical algorithms are RSA and others.

2.1 Data Encryption Standard (DES)

DES was designed by IBM in 1977. DES is a symmetric key cryptography algorithm. In DES, size of input block is 64-bits long and key is 56-bits long. Same key is used for encryption and decryption [2]. DES contains various operations such as mixing of bits, substitution, exclusive OR, S-boxes, straight permutation and expansion permutation [5][6]. The structure of DES is as shown in Figure 2 below.

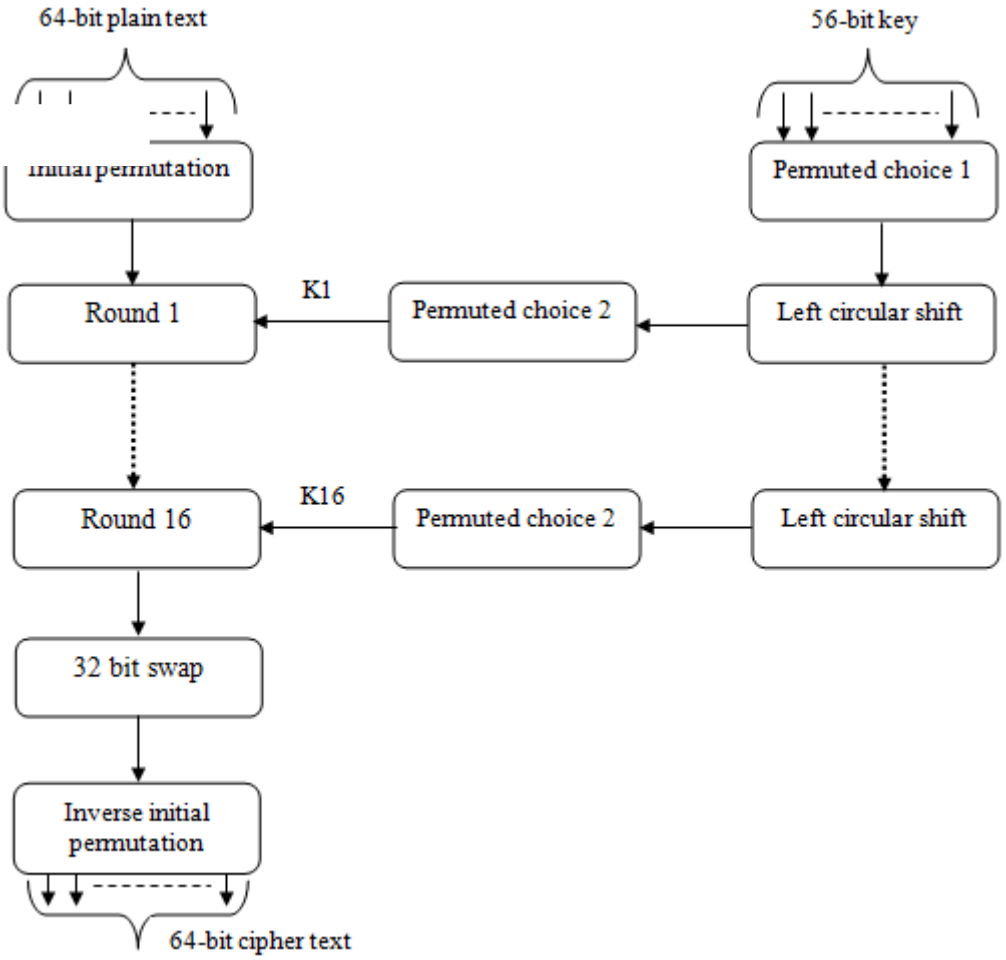

Figure 2: General description of DES algorithm

Initial Permutation (IP) block rearranges the bits to produce the permuted output. This step is followed by the phase involving 16 rounds of same function which again involves both permutation and substitution functions [1]. The output of last 16th round consists of 64 bits that are function of plaintext and the key. The right and left halves of the outputs are swapped to produce the preoutput. Finally this pre output is passed through inverse permutation function to produce 64 bit cipher text. The 56 bits key is passed through

a permutation function. Then, a subkey is produced for each of the 16 rounds by the combination of a left circular shift and a permutation. Same permutation function is used for each round but different subkey is produced because of the repeated iteration of the keys. Single round of DES algorithm is as shown in Figure 3 below.

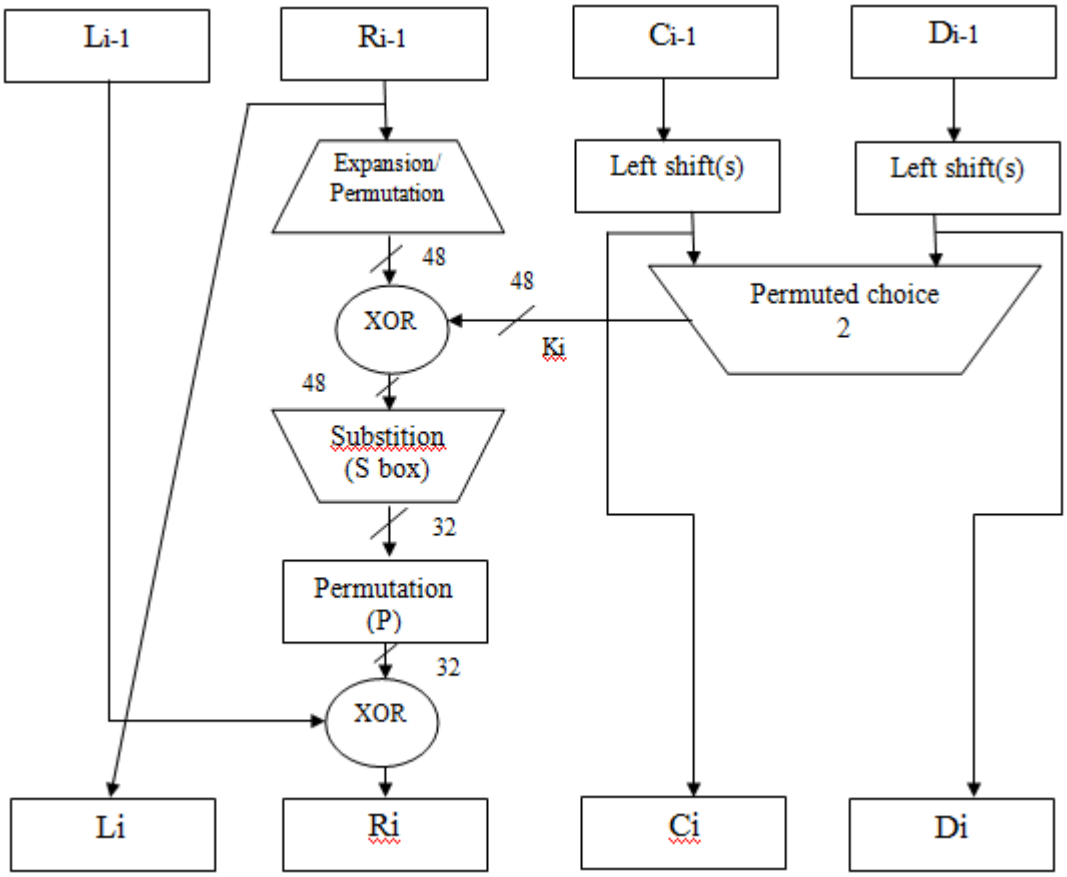

Figure 3: Single round of DES algorithm

The Single round of DES algorithm steps are as follows:

- ❖ DES accepts 64-bit long plaintext and 56-bit key (8-bit parity) as inputs and produces an output of 64-bit block.
- ❖ The plaintext block shifts the bits around.
- ❖ The 8 bits of parity are removed from the key by subjecting the key to its Key Permutation [6].
- ❖ The plaintext and key will be processed as follows,

- The key is divided into two 28 halves
- Each half of the key is shifted by one or more bits, depending on the round.
- The halves are joined together and subject to a compression permutation to reduce the key from 56 bits to 48 bits long. These compressed keys are used to encrypt this round's plaintext block.
- The shifted key halves from step 2 are used in next round.
- The data block is divided into two 32-bit halves.
- One half is subject to an expansion permutation to extend its size to 48 bits.
- Output of step 6 is XOR'ed with the 48-bit compressed key from step 3.
- Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back to 32-bits.
- Output of step 8 is further subjected to a P-box to permute the bits.
- The output from the P-box is XOR'ed with another half of the data block K. The two data halves are swapped and become the next round's input.

2.2 Triple Data Encryption Standard (3DES)

3DES is an enhancement of DES and it's block size is 64 bit with key size of 192 bits. In this algorithm the encryption method is similar to the one in the original DES and increase the encryption level and the average safe time [1]. It uses either two or three 56 bit keys in the sequence order of Encrypt-Decrypt-Encrypt. 3DES algorithm with three keys require 2^{168} combinations and with two keys require 2^{112} combinations and it is slower than other block cipher methods because it's too time consuming.

2.3 Advanced Encryption Standard (AES)

Advanced Encryption Standard **(**AES) was developed by Vincent Rijmen and Joan Daemen [1]. Because of the small key length the Data Encryption Standard (DES) is no longer considered as safe for today's applications. AES come up with key length of 128 bit long using the symmetric block cipher as shown in Figure 4. AES algorithm is not only for security but also for great speed. The encryption steps are as follows.

- The set of round keys from the cipher key.
- Initialize state array and add the initial round key to the starting state array.
- Perform round = 1 to 9: Execute Usual Round.
- Execute Final Round.
- Corresponding cipher text chunk output of Final Round Step.
- Encryption round consists of following steps.

  - ❖ Sub Bytes: The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.
  - ❖ Shift Rows: In the encryption, the transformation is called Shift Rows.
  - ❖ Mix Columns: The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.
  - ❖ Add Round Key: Add Round Key proceeds one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition.
  - ❖ The last step consists of XORing the output of the previous three steps with four words from the key schedule [6]. And the last round for encryption does not involve the "Mix columns" step.

a) Decryption involves reversing all the steps taken in encryption using inverse functions like a) Inverse shift rows, b) Inverse substitute bytes, c) Add round key, and d) Inverse mix columns. The last step consists of XORing the output of the previous two steps with four words from the key schedule. And the last round for decryption does not involve the "Inverse mix columns" step.

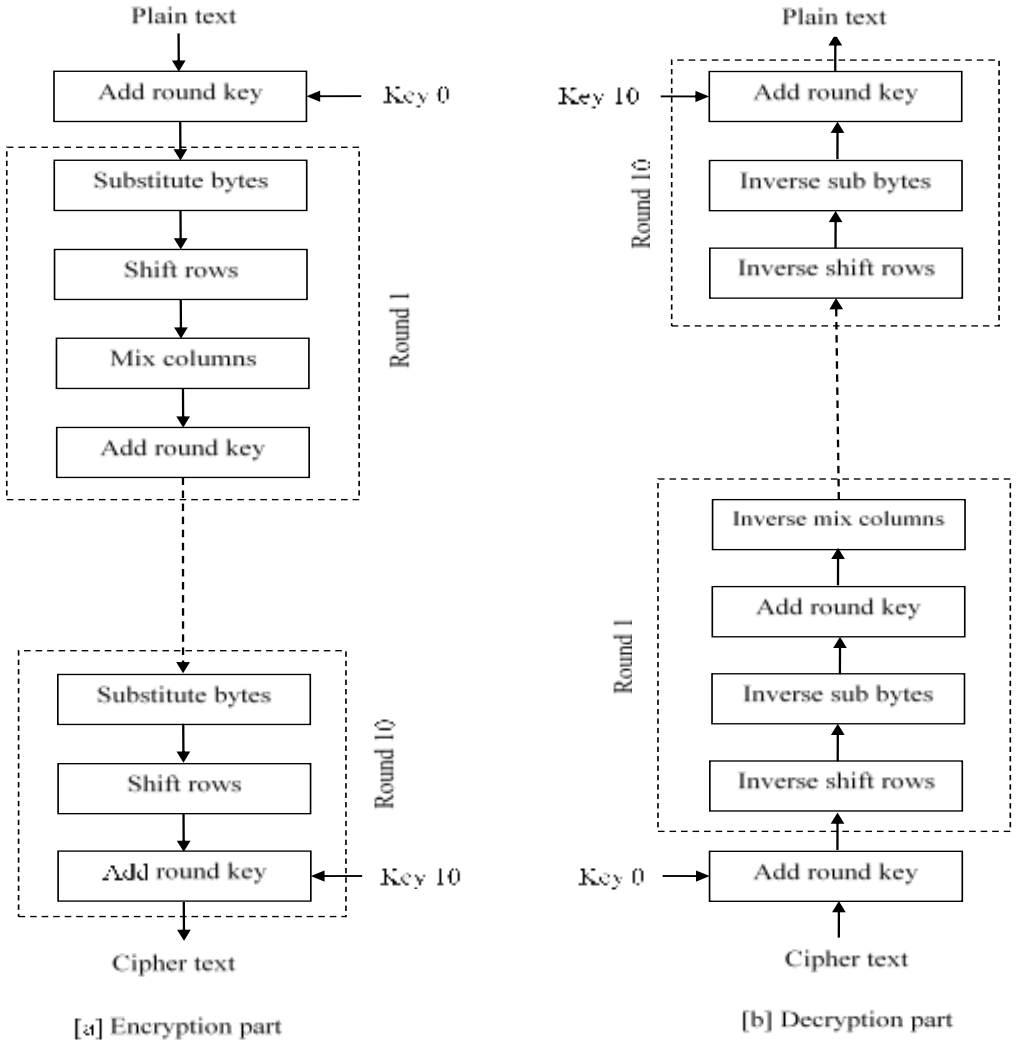

Figure 4 : AES Encryption and Decryption

2.4 Blowfish

Blowfish is a symmetric block cipher, designed by Bruce Schneier in 1993 [6]. The algorithm consists of two main parts: a key expansion part and a data encryption part. Blowfish includes a 64-bit block size and a variable key length from 32 up to 448 bits. Key expansion converts a key of at most 448 bits into many sub-key arrays totaling 4168 bytes. Blowfish follows sixteen rounds of Feistel Network. Bruce Schneier later created Twofish, that performs a similar function on 128-bit blocks [8][9]. The Blowfish is designed to aim four criteria known as Fast, Compact, Simple and Variably Secure. Blowfish has some categories of weak keys. For these weak keys, separate rounds end up using the same round-keys. Keys belonging to these categories can be detected only in reduced-rounds versions of the algorithm and not on the full blowfish.

2.5 RC5

RC5 is a symmetric key encryption algorithm [9]. It was designed by Ronald Rivest in 1994. RC stands for "Rivest Cipher" or it is also called as "Ron's Code". It uses block sizes of 32, 64 or 128 bits and 1 to 255 encryption rounds [6]. It is suitable for hardware and software implementation, because it uses only those operations which are available in typical microprocessor. A very stunning feature of RC5 is the use of data-dependent rotations. RC5 has a variable word size, a variable number of rounds, and a variable length secret key. The encryption and decryption algorithms are exceptionally simple. The RC5 can be represented as RC5 – w/r/b, For example, RC5 – 32/16/10 has 32-bit words, 16- rounds and a 10-byte (80-bit) secret key.

2.6 Rivest-Shamir-Adleman (RSA)

RSA [3] is a asymmetric key cryptography algorithm. It is named after the initials of it's discoverers, Ron Rivest, Adi Shamir and Len Adelman in 1977. It is the most popular public key cryptographic algorithm which provides both secrecy and digital signature. It makes use of the prime numbers to generate public and private keys based on mathematical calculations and multiplying large numbers together [5][11]. Steps involved in RSA algorithm are key generation, encryption and decryption.

- Key generation
  - Select p and q ; p and q both are prime numbers .
  - Calculate n = p x q
  - Calculate $\Phi(n) = (p-1) \times (q-1)$
  - Select integer e ; GCD [$\Phi(n)$, e] = 1
  - Calculate d ; $d = e^{-1} \mod (\Phi(n))$
  - Public key ; PU = {e, n}
  - Private key ; PR = {d, n}
- Encryption
  - Plain text : M < n
  - Cipher text : $C = M^e \mod n$
- Decryption
  - Cipher text : C
  - Plain text : $M = C^d \mod n$

For example,

- Choose p = 3 and q = 11
- Compute n = p x q = 3 x 11 = 33
- Compute $\Phi(n) = (p - 1) \times (q - 1) = 2 \times 10 = 20$
- Choose e such that $1 < e < \Phi(n)$ and e and $\Phi(n)$ are co-prime.
- Let e = 7
- Compute a value for d such that (d x e) % $\Phi(n)$ = 1. One solution is d = 3 [(3 * 7) % 20 = 1]
- Public key is (e, n) = (7, 33)
- Private key is (d, n) = (3, 33)
- The encryption of m = 2 is $c = 2^7 \% 33 = 29$
- The decryption of c = 29 is $m = 29^3 \% 33 = 2$

3. COMPARISION OF CRYPTOGRAPHIC ALGORITHMS

Table 1: Comparison of all above cryptographic algorithms

Algorithm	Created by	Year	Key size (in bits)	Block size (in bits)	Type	Features
DES	IBM	1977	64	64	Symmetric	Not Strong Enough
3DES	IBM	1978	112 or 168	64	Symmetric	Adequate Security
AES	Joan Daeman & Incent Rijmen	1998	128,192, 256	128	Symmetric	Replacement for DES, Excellent Security
Blowfish	Bruce Schneier	1993	32 or 448	64	Symmetric	Fast Cipher in SSL
RC5	Ronald Rivest	1994	128	32,64 or 128	Symmetric	Good Security
RSA	Rivest Shamir Adleman	1977	1024 to 4096	128	Asymmetric	Excellent Security and Low Speed

4. CONCLUSION

With the rapid growing of internet and networks applications, security of information becomes more important. Encryption algorithm plays very important role in information security. This paper gives a study of selected existing symmetric algorithms like DES, 3DES, AES, BLOWFISH, RC5 and asymmetric algorithm like RSA. All these techniques are useful for real-time encryption. Every technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence high speed and secure conventional encryption techniques will always work out with high rate of security.

5. REFERENCES

[1] William, Stallings. "Cryptography and network security: principles and practices." Pearson Education India, 2006.
[2] Mahajan, Prerna, and Abhishek Sachdeva. "A study of encryption algorithms AES, DES and RSA for security." Global Journal of Computer Science and Technology (2013).
[3] Al Hadi, Abdul Hai. "A survey on some encryption algorithms and verification of RSA technique." International Journal of Scientific & Technology Research 2, no. 12 (2013): 285-287.
[4] AbuTaha, Mohammed, Mousa Farajallah, Radwan Tahboub, and Mohammad Odeh. "Survey paper: cryptography is the science of information security." (2011).
[5] Bali, Priti. "Comparative study of private and public key cryptography algorithms: A survey." IJRET: International Journal of Research in Engineering and Technology (2014).
[6] Swathi S V, Lahari P M, Bindu A Thomas. "Encryption Algorithms: A Survey." International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016).
[7] Thambiraja, E., G. Ramesh, and Dr R. Umarani. "A survey on various most common encryption techniques." International journal of advanced research in computer science and software engineering 2, no. 7 (2012).
[8] Mona, M. Chanda, S. Banu Chitra, and V. Gayathri. "A Survey On Various Encryption And Decryption Algorithms." International Journal of Security (IJS) Singaporean Journal of Scientific Research (SJSR) Vol 6 (2014): 289-300.
[9] Yegireddi, Ramesh, and R. Kiran Kumar. "A survey on conventional encryption algorithms of Cryptography." In ICT in Business Industry & Government (ICTBIG), International Conference on, pp. 1-4. IEEE, 2016.
[10] Agrawal, Vikas, Shruti Agrawal, and Rajesh Deshmukh. "Analysis and review of encryption and decryption for secure communication." International Journal of Scientific Engineering and Research (IJSER) 2, no. 2 (2014).
[11] Saranya, Vinothini. Vasumathi,"A Study on RSA Algorithm for Cryptography." International Journal of Computer Science and Information Technologies 5, no. 4 (2014).

