A Study: Cryptology Techniques and Methodologies

Cutifa Safitri[1], Haroon Shoukat Ali[2], Jamaludin Bin Ibrahim[3]

Kulliyyah of Information and Communication Technology, International Islamic University Malaysia
Gombak, Malaysia

Abstract: ***Cryptography, as the most important aspect in the never ending evolving information technology era, is being criticized in its aspect. Information outbreaks make users doubtful on relying on their own information in current cryptosystems. This paper attempts to define the existing cryptology techniques and measures how strong and 'bullet proof' they are. In this paper, a basic encryption, byte to byte and complex encryption is shown as a study of cryptosystem classes that were used to overcome the need from various users. By understanding the current world phenomenon, it would be easier to answer the question of how secure cryptology actually is.***

Keywords: Information Security, Cryptosystems, Network Security, Cryptoanalysis, Cryptography.

1. Introduction

To understand the term cryptology we have to go back to 1935, where the term cryptology is first heard of. Cryptology, the practice and study of techniques for secure communication, concerned with the message / plain text confidentiality, integrity, non repudiation and authentication [1]. When dealing with cryptography techniques, always keep in mind that it will be broken. The idea is to find a way to go down with grace. Is cryptology broken? It is not the right question. The question is, how long is cryptology secured until it becomes broken? This paper attempts to define the existing cryptology techniques and measure how strong and 'bullet proof' they are. Later in this paper, a basic, byte to byte and complex encryption is shown as a study of encryption classes.

There are two types of encryption type, symmetric and asymmetric. The asymmetric cryptography technique, such as RSA, that relies in prime factorization is hard to be tempered. It is claimed that even if some of the utility numbers are compromised, the encryption is still intact. But, there is also an algorithm that gives disclosure to decryption key that attempt to compromise the ciphertext, such as Las Vegas algorithm that provide a quicker factorization to break RSA [2].

In cryptology, key size or key length, is the size in bits of the key used in a cryptographic algorithm. An algorithm's key length is distinct from its cryptographic security. The security of an algorithm cannot exceed its key length, but it can be smaller. Keys are used to control the operation of a cipher so that only the correct key can convert the encrypted text or ciphertext to plaintext. A key should therefore be large enough so that an attack on it can take a long time to decrypt.

Nowadays, we extent the number of encryption key digits, naively thinking, that raising key digits takes longer time and more power for attackers to decrypt it. Yes there is a super-speed and powerful computer machine that can take care of heavy encryption-decryption algorithm. But again, people are not willing to spent costs higher than the value of the message / the plain text itself.

Each encryption system has different cryptographic complexity. The actual degree of security achieved overtime varies, as more computer machinery power and more powerful mathematical methods become available. Hence, cryptologists tends to look at algorithms and key length as indicator signs of potential vulnerability and move to longer key size and more difficult algorithm.

2. Literature Review

Symmetric encryption is the older and more simpler method of encrypting information. The basis of symmetric encryption is that both the sender and the receiver of the message have previously obtained the same key. Below we describe a few symmetric key encryption techniques.

DES (Data Encryption Standard) was developed in 1973 by the National Bureau of Standard (NBS). DES is what is known as a block cipher, segmenting the input data into blocks of a specified size, typically padding the last block, making it multiple of the block size required. There have been multiple successful attacks against DES algorithms that use fewer rounds. Any DES with fewer than 16 rounds could be analyzed more efficiently with chosen plaintext that, via a brute-force attack uses differential cryptanalysis. With 16 rounds and not using a weak key, DES is reasonably secure, and amazingly has been for over 20 years[3].

3DES (Triple DES) is a variant of DES. Depending on the specific variant, it uses either two or three keys instead of the single key that DES uses. it also spins through the DES algorithm three times via multiple encryption. The only weaknesses of 3DES are the ones that already exist in DES, and due to the use of different keys in the same algorithm, resulting in a longer key length by adding the first keyspace to the second keyspace, and hence greater resistance to brute force. 3DES has less actual weakness. 3DES is a good interim step before the new encryption standard AES is fully implemented to replace DES[3].

AES (Advance Encryption Standard), called for a block cipher using symmetric key cryptography and supporting key sizes of 128, 192, and 256 bits. This new algorithm is well thought-out and has suitable key lengths to provide security for many years to come. While there are currently no efficient attacks against AES, more time and analysis will tell if this standard can last as long as DES has[3].

CAST (Carlisle Adams and Stafford Tavares), uses a 64-bit block size for 64- and 128- bit key versions, and a 128-bit block size for the 256-bit key version. It divides the plaintext block into a left half and a right half. CAST has been through thorough analysis with only minor weaknesses discovered that are dependent on low numbers of rounds. There is currently no better way known to break high round CAST than by brute forcing the key, meaning that with sufficient key length, CAST should be placed with other trusted algorithms[3].

RC (Rivest Cipher), has series of working algorithm names RC2, RC4, RC5 and RC6. RC2 was designed to be a DES replacement, and it is a variable key-size block-mode cipher. RC2 breaks up the input block into four 16-bit words, and then puts them through 18 rounds of one of two operations. According to RSA, RC2 is up to three times faster than DES. RSA maintained RC2 as a trade secret for a long time. the ability of RC2 to accept different key lengths is one of the larger vulnerabilities in the algorithm. Any key length below 64 bits can easily be retrieved by modern computational power[3].

In RC4, the algorithm is fast, sometimes ten times faster than DES. The most vulnerable point of the encryption is the possibility of weak keys. One key in 256 can generate bytes closely correlated with key bytes. RC6 is a modern algorithm that runs well on 32-bit computers. With sufficient number of rounds, the algorithm makes both linear and differential cryptanalysis infeasible. The available key lengths make brute-force attacks extremely time-consuming. RC6 should provide adequate security for some time to come[3].

Blowfish, was designed in 1994 by Bruce Schneier. Its a block-mode cipher using 64 bit blocks and a variable key length from 32 to 448 bits. It was designed to run quickly on 32-bit microprocessors and is optimized for situations where there are few key changes. The only successful cryptanalysis to date against Blowfish has been against variants that used reduced rounds. There does not seem to be weaknesses in the full 16-round version[3].

IDEA (International Data Encryption Algorithm), current cryptanalysis on full, eight-round IDEA shows that the most effective attack would be to brute force the key. The more increased bit key would prevent this attack from being accomplished. The only known issue is that IDEA is susceptible to a weak key- a key that is made of all zeros. This weak key is easy to check for, and the weakness is simple to mitigate[3].

Symmetric algorithms are important because they are comparatively fast and have fewer computational requirements. Their main weakness is that there is no function of key exchange, which is greatly facilitated by asymmetric key cryptography[3]. Asymmetric cryptography is more commonly known as public key cryptography. The system uses a pair of keys. a private key, one that is kept secret and a public key that can be sent to anyone[3].

RSA (Rivest, Shamir, Adleman) is one of the first public key cryptography algorithms ever invented and was published in 1977. This algorithm uses the product of two very large prime numbers and works on the principle of difficulty in factoring such large numbers. Since the security of RSA is based upon the supposed difficulty of factoring large numbers, the main weaknesses are in the implementation of the protocols. Until recently RSA was a patented algorithm, but it was a de facto standard for a many years[3].

Diffie-Hellman was created in 1976 and this protocol is one of the most common encryption protocol used today. It plays a role in the electronic key exchange method of the Secure Socket Layer (SSL) protocols. It is also used by the SSH and IPsec protocols. This protocol is important because it enables the sharing of a secret key between two people who have not contacted each other before. Though there have been methods to strengthen it, Diffie-Hellman is still widely used. It remains very effective because of the nature of what it is protecting, which is just a temporary automatically generated secret key that is only good for a single communication session[3].

ElGamal, by Taher Elgamal, was designed in the early 1980s. This system was never patented and is free for use. It can be used for both encryption and digital signatures. It is also used as the U.S Government standard for digital signatures. ElGamal is an effective algorithm and has been in use for sometime. It is used primarily for digital signatures. Like all asymmetric cryptography algorithms, it is slower than symmetric cryptography[3].

ECC (Elliptic Curve Cryptography), works on the basic of elliptic curves. An elliptic curve is simply a function that is drawn as a gently looping curve on the X, Y plane. for cryptography, the elliptic curve works as a public key algorithm. Users agree on an elliptic curve and a fixed curve point. The security of elliptic curve has been questioned, mostly because of lack of analysis. However, all public key systems rely on the difficulty of certain math problems. Research has been done about the problems and had shown that the elliptic curve problem has been more resistant to incremental advances[3]. Asymmetric encryption creates the possibility of digital signatures and also corrects the main weakness of symmetric cryptography. With strong algorithms and good key lengths, security can be assured[3].

There are other various cryptosystems that have not been mentioned here, such as Visual Cryptosystems. Visual Cryptography is a special encryption technique used to encrypt images in such a way that it can be decrypted by the human visual system in presence of the correct key images. This scheme enhances the security by encrypting with Public Key Cryptography, which provides the strong security to the transfer of secret information in form of images, printed text and handwritten material [4].

3. Cryptanalysis

In the previous section of this paper, we looked at the various major cryptology standards applied and used in various sectors of the world. In our research on how safe or broken the science of cryptology is, we need to look at both aspects of cryptology if we need to decide on its merits or demerits. This section presents a comprehensive overview of some of the cryptanalysis techniques that have been employed or researched, to attempt to crack the various cryptographic algorithms mentioned before. Gaining an understanding of these techniques helps us evaluate the safety and sturdiness of the encryption algorithms, and it also helps us to see a pattern of cryptanalysis over the years.

The DES cipher has been subjected to cryptanalysis attacks, with success on many occasions in the past. Two main methods have been researched here - Linear Cryptanalysis and Differential Cryptanalysis. The linear cryptanalysis method consists mainly of known-plaintext attacks. Researchers have reached several successful conclusions when it comes to breaking DES ciphers [9]. It was found out that,

- 8-round DES breaks with 2^{21} plaintexts in 40 seconds
- 12-round DES breaks with 2^{33} plaintexts in 50 hours
- 16-round DES breaks with 2^{47} plaintexts with a speed higher than an exhaustive search for 56 key bits

The differential cryptanalysis of DES suggested by other researches, has the capability of breaking an 8-round DES within a few minutes, and a 15-round DES in around 2^{56} operations. The DES cipher first came into existence in the year 1977, and successful theories of its first cryptanalysis were proposed in 1991 [10].

A handful of exploits have also been discovered and researched on, for the triple-DES algorithm. The first among these is what is known as *meet-in-the-middle* attack. A further successful method of cryptanalysis for triple-DES was proposed in the years following the discovery of the first attack. The most successful among these used s^{32} known plaintexts, 2^{113} steps, 2^{90} single DES encryptions and 2^{88} memory [11]. Research has also suggested another successful attack scheme on the 3DES, which follows the method of neuro-cryptanalysis. It is a known-plaintext attack, which is based on training a neural network to do the decryption process without knowing the key [12]. One of the first successful attacks on the 3DES was proposed in the same year of its invention, in 1998. The Advanced Encryption Standard (AES) is sought by many to be one of the strongest cryptography algorithms, with very few breaking mechanisms discovered. The cryptanalysis mechanisms, even if discovered, were deemed impractical with respect to time. The first breakthrough came in 2002, when a theoretical attack, other than a brute-force, on AES was announced [13]. Following this, a better, more hopeful attacking scheme on AES was discovered and presented in 2002. This was applicable to AES-192 as well as AES-256 standards. Both of these were boomerang attacks, which are based on the idea of finding local collisions in block ciphers [14]. One of the most successful and recent discovered attacks on full AES use Biclique Cryptanalysis techniques [15]. These have resulted in the following findings:

- Recovery attack on full AES-128, complexity $2^{126.1}$
- Recovery attack on full AES-192, complexity $2^{189.7}$
- Recovery attack on full AES-256, complexity $2^{254.4}$

The AES standard was introduced first in 1998, with the first research and news of cryptanalysis on it emerging in 2002. When it comes to the CAST cipher, not many cryptanalysis techniques, other than plain brute force have been proposed. It is currently regarded as a secure cipher algorithm. However, there has been research on breaking a CAST cipher with 5 rounds. The proposed mechanism here is a higher order differential attack, which would help recover the last round key of a CAST cipher with 5 rounds, provided it uses 2^{17} known plaintexts, in around 15 seconds on an UltraSPARC station [16]. The CAST cipher was discovered in the year 1996, with its first theoretical exploit being published in the year 1998.

The Rivest Cipher group of ciphers (RC2, RC4) have had some theories of breaking them over the last decade. For RC2, researches have proposed a related-key cryptanalysis technique which breaks RC2 with around one related-key query and 2^{34} chosen plaintexts[17]. While RC4 remains a very secure cipher for practical applications, several theories have been suggested for breaking it, but none of them are considered successful against commonly used key lengths. One of them is a method of Tracking Cryptanalysis, which result in reducing complexity of the RC4 algorithm, and provide a significant improvement over brute-force type methods for RC4. Using this, the state of a 5 bit C4-like cipher can be obtained from a part of a keystream in 2^{42} steps [18]. One of the latest and most clever attacks on the RC4 cipher was discovered on March 29, 2013. This is mainly an attack against TLS that use the RC4 encryption. The attacks arise from statistical flaws in the keystream generated by the RC4 algorithm which become apparent in TLS ciphertexts when the same plaintext is repeatedly encrypted at a fixed location across many TLS sessions. This cipher was first introduced in 1987, with the first few cryptanalysis theories originating in 1999.

The blowfish cipher has no known effective cryptanalysis techniques reported. However, there has been a recent research into this, and a few weak keys for the Blowfish cipher have been discovered. The research described reflection attacks on r-round blowfish ciphers. The amount of keys on which these attacks work successfully, however, are very limited, termed by the researchers as *reflectively weak keys* [19]. The blowfish cipher was first discovered in 1994, with the first few weak keys being discovered in the year 2007.

With regards to the IDEA cipher, amongst the first effective attack theories, other than brute force, were proposed in 1993, which present a differential attack on 2 and 5 rounds of IDEA. These require 2^{10} chosen plain text encryptions. The said attack was proposed to be very powerful against IDEA [20]. Another breakthrough was proposed a few years later, which was described as a Key-Schedule cryptanalysis of IDEA cipher. This attack was based on related-key differential cryptanalysis, which allow keys as well as plain texts with specific differences to be chosen. It is proposed here, that IDEA has a simpler key-schedule, and the researchers use this to describe an attack on 3-round IDEA. The attack is said to recover 32 bits of key using two plaintexts under the first key and four under the second [21]. The latest and best breakthrough for IDEA cracking has been in the form of a high order differential attack requiring 2^{64}-2^{52} chosen plaintexts, which can break 6 rounds with a computational complexity of $2^{126.8}$.

The RSA cryptosystem, from its creation in 1977, has been tested on, and subjected to many attacks to analyze its vulnerable areas. Among the numerous cryptanalysis techniques used to exploit RSA, some of the notable ones include Factoring, Low Private Exponent Attack, Partial Key Exposure Attack, Broadcast and related messages attacks, Short Pad Attack, Implementation Attack and Timing Attack [22]. Amongst these and many other attacks, the first attacks on the RSA cryptosystem have been believed to have been conducted in the mid 80s[23].

The ElGamal scheme has been subjected to a few cryptanalysis techniques. One of them involves Fault Cryptanalysis, which can help in recovering a key with a probability of 0.5, after nlog2n error sightings and with a complexity of O(n^{2}logn) [24]. ElGamal system first came into existence in the 1980s. This attack has been discussed and proven around 2005. From the above studies on cryptanalysis on some cryptography methods, it can be observed that almost any method has some kind of weakness associated with it, which is discovered in the years following its release. It is important to note here however, that many of these exploits and weaknesses are theoretical at the time of discovery, primarily due to absense of practical machinery or time period which would deem these methods successful in practive. Neverthless, the focus on the discussion here is to show that weaknesses in any cryptology system exist in theory, and this would indicate that there is no system which is free of any attacks, exploits or weaknesses par se.

The following graph presents a visual overview of the approximate time in years, it has taken, for exploits and cryptanalysis techniques to be discovered, for most of the big cryptology mechanisms discussed above.

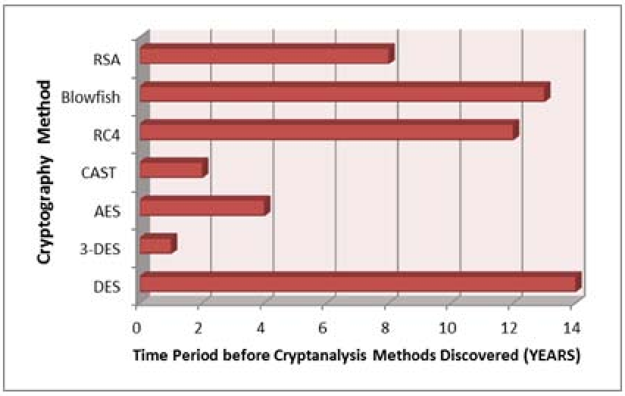


Figure 1: Visual overview of Cryptanalysis over time

4. Discussion

Cybercrime is defined as any offense committed using a computing device, personal computer and computer networks, including smartphones [5]. Cybercrime is simply a more high-tech version of old 'real-world' crimes. Thus, any crimes committed to break cryptography is an old fashioned crime to gain any valuables, or in this case, valuable information. Why do people attack? The attempt to break an encryption may be motivated by hatred against government or any organization. This era is motivated to launch an attack with more effective and cheaper methods. For instance, taking out a country's water supply system is more effective than dropping plane-loads of bombs with expensive rockets. Any unauthorized entry into telecommunication systems or messages, is considered an intellectual crime. Some do it for the thrill, and others are motivated by money.

Mathematicians build a range for strong encryption method. They are varied so people can choose the encryption that suits their needs. However, in the past, every known encryption is believed to be ssociated with some form of known attack. Some of the methods that have been proposed to fight back are by having a joint co-operation project, such as MARS (Microsoft Active Response for Security) and using various combination strategies with technology end-people and authorities end-people [5].

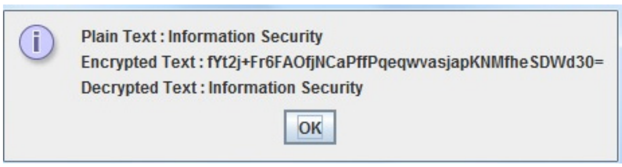
Some governments implement Key Escrow - a system by which the private key is kept both by the owner and government - thus the key can be retrieved by court order. At first this Key Escrow was implemented to keep a safe place for all private keys, also to watch the 'watcher'. The drawback is that, once any break in or attack is launched against the key storage, all the keys are unleash into the world [3].

In the never ending race between hackers and cryptography, quantum mechanics seemed to be the potential winner. Quantum cryptography allows us to encrypt a message in a way such that it cannot be read by any code breakers or hackers. Quantum cryptography promises to revolutionize secure communication by providing security based on the fundamental laws of physics. In quantum cryptography the secret key is encrypted into a series of photons and can be passed between two parties trying to share secret information. But again, quantum cryptography does not provide any protection against the classic bucket brigade attack (man in middle attack). The signal is limited, thus its vulnerable if the man in the middle blinds a photons detector with heavy and strong pulses, rendering it to see the secret keeping photons [6].

The current standard cryptography suffers from side channel attack as well as social engineering [7]. Thus, there is indeed a need of unique encryption that is defined from a unique and more sophisticated approach. The function should also be fast, low cost, simpler, user friendly and should consume small amount of resources. In addition, it also must have important characteristics such as appearing as an unknown value and the characteristic of unpredictability. Confidentiality in cryptography is gained because encryption is very good at scrambling information to make it look like random noise, when in fact a key can decipher the message and return it to its original state. A strong cryptosystem is considered strong only until it's been cracked. Although that may sound like common sense, one can never prove that a cryptosystem is strong. Each defect of an attempt to crack a cryptosystem serves to strengthen the belief in its ability to secure. A cryptosystem has value because its user believes in its worth [8]. Once that worth is proven to be wrong, the cryptosystem collapses and no one relies on it anymore. This paper is also attempts to present a study from experience gained from various cryptography classes. The idea is to prevent attacks on zero knowledge protocol and increased complexity of encryption techniques. The aim is the minimalism of prediction, hence it will be more difficult to break in the attempt to attack. This part will cover on simple encryption, a byte to byte encryption, and a more sophisticated encryption.

4.1 Basic Encryption

Every user has their own level of needs and the information they wish to encrypt. The user with high mobility might require a lightweight program, a simple encryption might suffice their need.

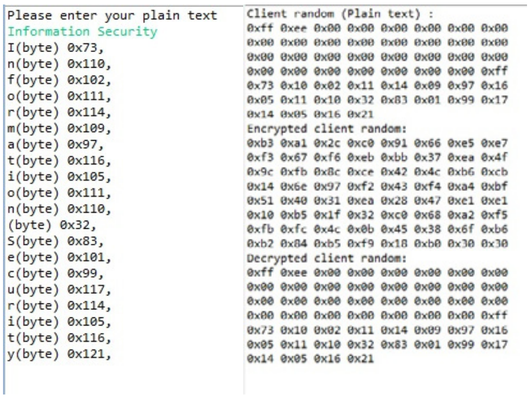


Plain Text : Information Security
Encrypted Text : fYt2j+Fr6FAOfjNCaPffPqeqwvasjapKNMfheSDWd30=
Decrypted Text : Information Security

Figure 2: Basic Encryption

4.2 Byte level Encryption

A byte level encryption hardens the information security by having the information scattered into byte to byte form. In this condition, if there is any attack attempted on the information, they might only get parts of the byte and will lead into segmented meaningless information.



```
Please enter your plain text
Information Security
I(byte) 0x73,
n(byte) 0x110,
f(byte) 0x102,
o(byte) 0x111,
r(byte) 0x114,
m(byte) 0x109,
a(byte) 0x97,
t(byte) 0x116,
i(byte) 0x105,
o(byte) 0x111,
n(byte) 0x110,
(byte) 0x32,
S(byte) 0x83,
e(byte) 0x101,
c(byte) 0x99,
u(byte) 0x117,
r(byte) 0x114,
i(byte) 0x105,
t(byte) 0x116,
y(byte) 0x121,
```

```
Client random (Plain text) :
0xff 0xee 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0xff
0x73 0x10 0x02 0x11 0x14 0x09 0x97 0x16
0x05 0x11 0x10 0x32 0x83 0x01 0x99 0x17
0x14 0x05 0x16 0x21
Encrypted client random:
0xb3 0xa1 0x2c 0xc0 0x91 0x66 0xe5 0xe7
0xf3 0x67 0xf6 0xeb 0xbb 0x37 0xea 0x4f
0x9c 0xfb 0x8c 0xce 0x42 0x4c 0xb6 0xcb
0x14 0x6e 0x97 0xf2 0x43 0xf4 0xa4 0xbf
0x51 0x40 0x31 0xea 0x28 0x47 0xe1 0xe1
0x10 0xb5 0x1f 0x32 0xc0 0x68 0xa2 0xf5
0xfb 0xfc 0x4c 0x0b 0x45 0x38 0x6f 0xb6
0xb2 0x84 0xb5 0xf9 0x18 0xb0 0x30 0x30
Decrypted client random:
0xff 0xee 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0xff
0x73 0x10 0x02 0x11 0x14 0x09 0x97 0x16
0x05 0x11 0x10 0x32 0x83 0x01 0x99 0x17
0x14 0x05 0x16 0x21
```

Figure 3: Byte to Byte Encryption

4.3 Unique Encryption

For the more enhanced user and more sophisticated user, a larger amount of bytes of encryption is needed. The encryption value will be generated without depending on how large the original plain text is. Strong cryptosystems produce ciphertext that always appears random to standard statistical test. It also resists all known attacks on cryptosystems and these have been brutally tested to ensure their integrity [8].

Figure 4: Unique Encryption

5. Conclusion

Ensuring a strong cryptographic system is certainly not an easy task. Still, it is something that many researchers have probably aimed to achieve as they want to protect their information against new launched attacks for a safer information system. This article has shown an understanding of the cryptosystems available. It also focused on the fundamental concepts and techniques, insisting on the alternatives to have a more unique but also sophisticated encryption class. More details are presented in the literature.

6. Future Work

Several important problems remain to be investigated in the future study. Examples are the integration of complex objects (non-latin characters), conflicts of ASCII, and algorithm databases. Theoretical work is also needed for new cryptographic systems. It is therefore important that efforts to solve the 'broken' state of cryptology be continued and evaluated through experiments with real applications.

References

[1] Menezes, A. J., Van Oorschot, P. C., Vanstone, S. A., Handbook of Applied Cryptography ISBN 0-8493-8523-7

[2] Garret, J. Making, Breaking Codes: An Introduction to Cryptology. Prentic-Hall, Inc. United States of America. 2001.

[3] Conklin et al, Principles of Computer Security: Security+ and Beyond, 1st. Edition McGraw Hill, 2005

[4] Kaur, K.; Khemchandani, V., "Securing Visual Cryptographic shares using Public Key Encryption," *Advance Computing Conference (IACC), 2013 IEEE 3rd International* , vol., no., pp.1108,1113, 22-23 Feb. 2013

[5] Warren, P., Streeter, M. "Cyber Crime & Warfare: All That Matters", McGraw-Hill, US, 2013

[6] Kumar, R., Jinjwadiya, R., Kumar, D., Gupta, S. Quantum Cryptography: A Security Tool in Secure Transferring Data International Journal of Research in Computer Engineering and Electronics, Pg 3 Vol.2 Issue 3. June, 2013

[7] Shamsudin, AF., Suhaimi, MA., Makarin, RH., and Jaafar, AD, Unique class encryption (UCE) substitution boxes (S-Boxes) using mysterious Quranic for block ciphers in ICT security. In: IIUM Research, Innovation & Invention Exhibition (IRIIE 2010), 26 - 27 January 2010, Kuala Lumpur

[8] Merkow, M. S., Breithaupt, J., Principles of Information Security. Person Education, Inc., Upper Saddle River, New Jersey, 2006.

[9] Matsui, M. "Linear Cryptanalysis Method for DES Cipher". *EUROCRYPT '93-Lecture notes in Computer Science*. vol. 765, pp. 386-397. 1994.

[10] Biham, E., Shamir, A. "Differential cryptanalysis of DES-like cryptosystems". *Journal of Cryptology*. vol. 4, no. 1, pp3-72.1991.

[11] Lucks, S. "Attacking Triple Encryption". *Lecture Notes in Computer Science*. vol. 1372, pp. 239-253. Springer Berlin Heidelberg. 1998.

[12] Alani, M., M. "Neuro-Cryptanalysis of DES and Triple-DES". *Lecture Notes in Computer Science*. vol. 7667, pp. 637-646. Springer Berlin Heidelberg. Nov. 2012.

[13] Schneier, B. *Crypto-Gram Newsletter*. 15 Sept., 2002.

[14] Biryukov, A., Khovratovich, D. "Related-Key Cryptanalysis of the full AES-192 and AES-256". *Lecture Notes in Computer Science.* vol. 5912, pp. 1-18. Dec. Springer Berlin Heidelberg. 2009.

[15] Bogdanov, A., Khovratovich, D., Rechberger, C. "Biclique Cryptanalysis of the full AES". *ASIACRYPT 2011-Lecture notes in Computer Science.* vol. 7073, pp. 344-371. Springer Berlin Heidelberg. 2011.

[16] Moriai, S., Shimoyama, T., Kaneko, T. "Higher order differential attack of a CAST cipher". *Lecture Notes in Computer Science*. vol. 1372, pp. 17-31. Springer Berlin Heidelberg. 1998.

[17] Kelsey, J., Schneier, B., Wagner, D. "Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA". *Information and Communications Security*. pp. 233-246. 1997.

[18] Mister, S., Tavares, S. E. "Cryptanalysis of RC4-like Ciphers". *Lecture Notes in Computer Science.* vol. 1556, pp. 131-143. Springer Berlin Heidelberg. 1999.

[19] Kara, O., Cevat, M. "A new class of Weak Keys for Blowfish." In *Fast Software Encryption*, pp. 167-180. Springer Berlin Heidelberg, 2007.

[20] Daemen, J., Govaerts, R., Vandewalle, J. "Cryptanalysis of 2, 5 Rounds of IDEA". *ESAT-COSIC Report*. pp. 94-1. 1993.

[21] Kelsey, J., Schneier, B., Wagner, D. "Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES". *CRYPTO'96-Lecture Notes in Computer Science*. vol. 1109, pp. 237-251. Springer Berlin Heidelberg. Jan.,1996.

[22] Cid, C. F. "Cryptanalysis of RSA: A Survey". *Information Security Reading Room*. SANS Institute. 2003.

[23] Boneh, D., Rivest, R., Shamir, A., Adleman, L. "Twenty years of attacks on the RSA cryptosystem". *Notices of the AMS*, vol.46, no.2, 203-213. 1999.

[24] Biernat, J., Nikodem, M. "Fault cryptanalysis of ElGamal Signature Scheme". *EUROCAST 2005-Lecture Notes on Computer Science.* vol. 3643, pp. 327-336. 2005.

Author Profile

Cutifa Safitri received her B.CS (honours) from International Islamic University Malaysia in 2011 and currently enrolled in the M.IT program at Kulliyyah of Information and Communication Technology, International Islamic University Malaysia.

Haroon Shoukat Ali received his B.CS (honours) from International Islamic University Malaysia in 2011 and currently enrolled in M.IT program at Kulliyyah of Information and Communication Technology, International Islamic University Malaysia.

Jamaludin Bin Ibrahim is a senior academic fellow and adjunct professor at Kulliyyah of Information and Communication Technology, International Islamic University Malaysia. He is also certified for British Standard Institute ISO270001 Information Security Management System Lead Auditor.