Scientific and Practical Cyber Security Journal (SPCSJ) 1(2):60-68
Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667

CRITICAL ANALYSIS OF SOME CRYPTOGRAPHY ALGORITHMS

E. Jincharadze

Georgian Technical University

ABSTRACT

Nowadays large amounts of data are being transferred over different network channels that could be both public and private. Protecting information is more vital than ever. One of the main problems during transferring data is to ensure security. Nowadays the exchange of valuable information over Internet, such as bank transactions, credit card numbers and telecommunication services are already common practices. Because the world becomes more connected and communication methods are developed, the security on electronic services has become more important. In order to protect valuable data in computer and communication systems from unauthorized attack and modification different security methods must be involved. Cryptography is one such method to make sure that confidentiality, authentication, integrity, availability and identification of user data can be secured. Cryptography provides security and privacy of used data. Encryption is the process of converting normal data or plaintext to something incomprehensible or cipher-text by applying mathematical transformations or formulae. These mathematical transformations or formulae used for encryption processes are called algorithms.

At the present time, cryptography plays important role to provide security communication between multiple objects. In many modern studies, researchers are trying to identify best cryptography mechanisms with their strong and weak points in terms of their performance results. To select cryptographic technique according to a particular situation is not so easy task. To solve this issue we have to understand that technique selection is totally dependent on desired quality attributes such as efficiency and security.

In this paper is presented critical analyze of some cryptography algorithms DES, 3DES, AES, Blowfish and RSA is presented. According to the literature review we have analyzed the performance and efficiency of those algorithms. To make an evaluation of those systems was explained imitations of sample context. We have analyzed various encryption algorithms on the basis of different parameters and compared them to choose the best data encryption algorithm so that we can use it in our future work.

Introduction

Cryptography is the discipline that studies the mathematical techniques which are related to information security such as providing the security services of confidentiality, data integrity, authentication and nonrepudiation. The art and science of keeping messages secure is cryptography, and it is practiced by cryptographers [1]. More generally, cryptography algorithm is the technique or some formula that makes data or network secure by providing security. Cryptosystems are complex combinations of hardware and software used to transform plaintext messages into a series of unintelligible characters known as cipher text, then back to their original plaintext known as cipher text, then back to their original plaintext form. "An encryption algorithm scrambles data by combining the bits in the key with the data bits; in decryption, the algorithm unscrambles data by separating the data bits from the key bits." [3]. Cryptography is the science which ensures that information is sent in such secure way that the only person able to retrieve this information is the intended recipient. Contemporary cryptography is unable to meet the requirements, in that its use would impose such severe inconveniences on the system users, as to eliminate many of the benefits of teleprocessing [6].

Cryptography falls into two important categories: secret and public key cryptography. Both categories play their vital role in modern cryptographic applications. For several crucial applications, a combination of both secret and public key methods is indispensable [7].

There is some basic terminology used in cryptography, which we should know for better understanding of encryption algorithms. This terminology is very important to understand because in every algorithm description. Those common terms are**:** **Plain Text** - The original text or message used in communication in called as Plain text. **Cipher Text -** The plain text is encrypted in un-readable message. This meaningless message is called Cipher Text. **Encryption -** is a process to convert Plain text into Cipher text. This converted text can securely be transferred over the unsecure network. Encryption process is done using encryption algorithm. **Decryption -** Decryption process is the reverse of Encryption process. So we have simple function E(M)=C, D(C)=M, D(E(M))=M. **Key** is a numeric or Alpha-numeric text (mathematical formula). In encryption process it takes place on Plain text and in decryption process it takes place on cipher text. **Key size** is the measure of length of key in bits, used in any algorithm. **Block Size** - Key cipher works on fixed length string of bits. This fix length of string in bits is called Block size. This block size depends upon algorithm. **Round** of encryption means that how much time encryption function is executed in complete encryption process till it gives cipher text as output.

Cryptography has some goals that need to be ensured for user's information security. Modern cryptography concerns itself with the following four services. Let us now see the possible goals intended to be fulfilled by cryptography. **Confidentiality** is the fundamental security service provided by cryptography. It is a security service that keeps the information from an unauthorized person. It is sometimes referred to as privacy or secrecy. **Data Integrity** It is security service that deals with identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidently. Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user. **Authentication** provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender. **Non-repudiation -** It is a security service that ensures that an entity cannot refuse the ownership of a previous commitment or an action. It is an assurance that the original creator of the data cannot deny the creation or transmission of the said data to a recipient or third party.

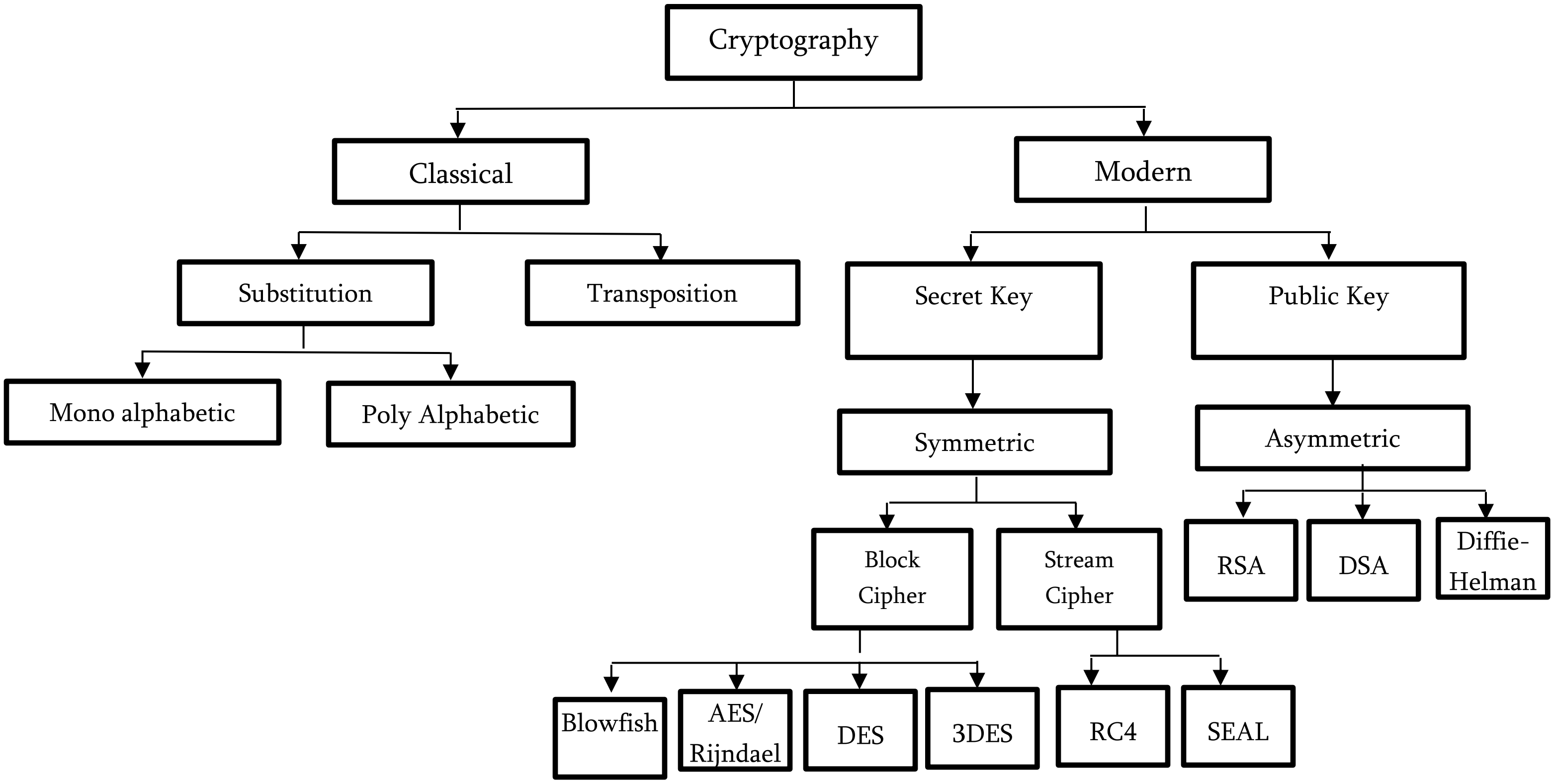

Figure 1. General overview of cryptographic techniques.

There are number of different encryption techniques which can be broadly divided into two categories: Symmetric Key Encryption and Asymmetric Key Encryption.

Symmetric algorithms, sometimes called conventional algorithms, are algorithms where the encryption key can be calculated from the decryption key and vice versa. In most symmetric algorithms, the encryption key and the decryption key are the same. These algorithms, also called secret-key algorithms, single-key algorithms, or one-key algorithms, require that the sender and receiver agree on a key before they can communicate securely [1]. Encryption and decryption with a symmetric algorithm are denoted by: $E_K(M) = C$, $D_K(C) = M$. In Symmetric key Encryption same key is used to encrypt and decrypt data. Receiver uses the same key and the corresponding decryption algorithm to decrypt the data. At the same time symmetric key cryptography is classified into two categories –Stream Ciphers and Block Ciphers. A stream cipher breaks the plaintext M into consecutive characters or bits, so we have following consequence m_1 , m_2 ,.. m_i. And each m_i is encrypted with k_i key, where K= k_1 , ... , k_i. So we have following equation $E_K(M)=E_{k1}(m_1)$ $E_{k2}(m_2)$ … $E_{ki}(m_i)$.

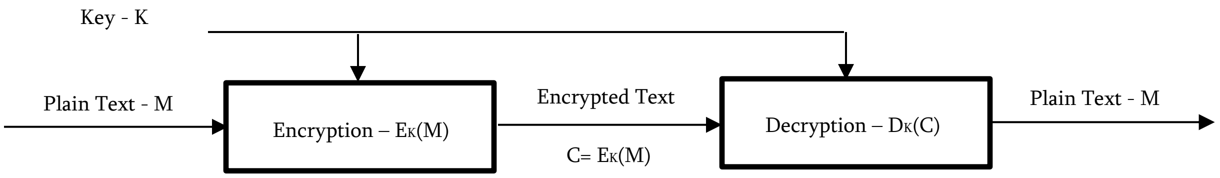

Figure 2. Symmetric key Cryptography

Asymmetric Key Encryption uses two different keys: public and private keys. Public key for encryption purpose and private key for decryption. Asymmetric Cryptography is cryptographic system which requires two separate keys K_E and K_D, where $K_E \neq K_D$. K_E is user to encrypt the plaintext - M, and K_D is used to decrypt the cipher text - C. Encryption key is published or public and the decryption key is kept private. Public key algorithms, unlike symmetric key algorithms, do not require a secure initial exchange of secret keys between the parties [2]. Public-key cryptography is a method which assures the confidentiality, authenticity of digital communications and data storage.

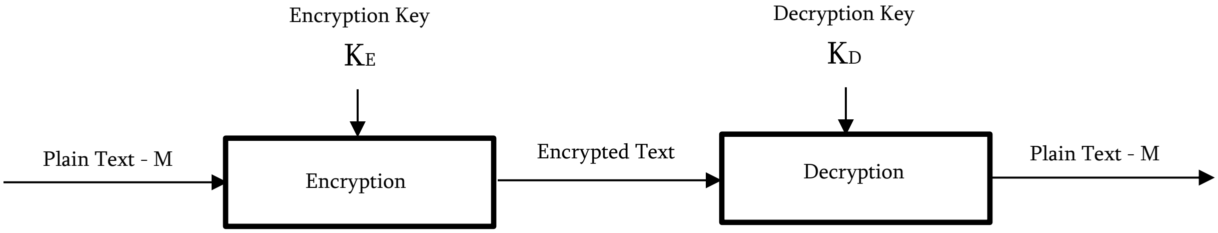

Figure 3. Asymmetric key Cryptography

OVERVIEW OF SOME CRYPTOGRAPHIC ALGORITHMS

There are many different types of cryptography algorithms. In this topic is described some of them and is analyzed each of them by terms of their usage and vulnerability. Is analyzed those algorithms performance for their evaluation. All of these algorithms are unique on it's way. However, the problem is that how to find the best security algorithm which provides the high security and also take less time for a key generation, encryption, and decryption of information. Security algorithms will depend on pros and cons of each algorithm, requirement and suitable for different application [13].

Data Encryption Standard (DES) – is a symmetric (secret key) block cipher algorithm, which was published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). DES is a block cipher that enciphers 64-bit blocks of data with a 56 bit key. The other 8 bits are used for checking correspondence. DES algorithm for decryption uses the same structure as encryption but with the keys used in reverse order. This is the advantage of DES algorithm because the same hardware or software can be used in both directions. But because of short key length DES is weaker about attacks. DES was approved in 1974 since that time many attacks were reported, which has made DES as insecure algorithm, so that DES could be broken under a known-plaintext attack by exhaustive search. It was also experienced that a special purpose machine consisting of a million LSI chips could try all 256 ≈ 7 X 10 16 keys in 1 day [1][3][7]. DES is not an ideal encryption technique in modern cryptography, instead it is used in mode of operation. The key length of DES system is 56 bits, that means that only 56 bits are actually used in the algorithm. So it means that we need maximum of 2^{56} attempts to find the correct key [14].

The weak point on DES attack is Brute force attack. DES' another weak point is it's slow encryption speed.

Triple-DES (3DES) – is one of the block cipher methods of symmetric key cryptography. 3DES was designed to improve weak points of DES but it is not totally different form DES. Triple DES is considered to be DES- three times. 3DES increases the key size from 56 bits to 168 bits to make it resistant from brute-force attack. It has two variants: one with two keys and other with three keys.

The negative side of 3DES is that it is slower than other block encryption methods, but it is more secured because of longer key length as it reduces many attacks. The strong side of 3DES algorithm is that it is three times secured than DES that's why it is better than DES encryption algorithm. 3DES provides security to the data but it is not the best because it consumes lot of time.

***Advanced Encryption Standard (AES)* -** is a symmetric block cipher, is also known as Rijndael algorithm and it was developed by NIST in late 90's. Was developed to protect classified information and is implemented in software and hardware throughout the world for sensitive data encryption. AES is actually, three block ciphers, AES-128, AES-192 and AES-256. 56-bit key of DES was not safe against the brute force attack and 64-bit blocks and was weak. AES encrypts data blocks of 128 bits using variable key length of 128,192 or 256 bits in 10, 12 or 14 rounds depending upon the key size [1] [3] [4]. In Advanced encryption standard there are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys[21]. The AES algorithm holds a 4 by 4 array of bytes called the state, that is initialized to the input of 128 bits (i.e., 16 bytes) to the cipher. The substitution and permutation operations are all applied to the state array. Each round of AES consists of four operations. AES can be implemented in small devices for encrypting a message to send over a network. Some other applications are monetary transaction and security applications [13] [16].

Blowfish is a symmetric block cipher algorithm. Blowfish uses the same secret key to both encryption and decryption of messages. Blowfish has block with 64 bits size. It uses a variable – length key, from 32 bits to 448 bits. Blowfish was developed by Bruce–Schneider in 1993 as an alternative to the existing encryption algorithms. It is appropriate for applications where the key is not changed frequently. It has 16 or less rounds. It is considerably faster than most encryption algorithms when executed in 32-bit microprocessors with huge data caches.

Blowfish provides good encryption and for this moment there is not known any attack to be successful against Blowfish. It is much faster than DES. But weak point of Blowfish algorithm is the weak key.

Rivest-Shamir-Adleman Algorithm – RSA is an asymmetric cryptographic algorithm which is used for encryption and decryption of the plain text. RSA is usually used in transferring of keys over an insecure channel. Because of that RSA is asymmetric algorithm, there are two keys used in the algorithm. In RSA, the encryption key is public and differs from the decryption key which is kept secret [1]. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. RSA provides confidentiality, integrity, authenticity, and nonrepudiation of data [1] [2]. RSA is more commonly used in electronic industry for online money transfer [19].

In RSA cryptographic algorithm the main disadvantage is its encryption speed, because for encryption it consumes lot of time. Generally this is disadvantage of asymmetric key algorithms because the use of two asymmetric keys. RSA provides good level of security but the same time it is slow for encrypting files. Another weak point of this algorithm is usage of fake key at decryption level. For successful encryption the secret key should be private and correct.

LITERATURE SURVEY

According to the different literature survey we could say that encryption algorithms AES showed poor performance results compared to other algorithms as it requires more processing power. The comparison also reveals that 3DES requires always more time than DES because of its three phase encryption technique.

Hamdan O. Alanazi made a comparison of three symmetric block ciphers DES, 3DES and AES on nine parameters. They got following result DES is vulnerable to brute force attack and no more secure as the 56 bit key space. It is possible to calculate DES with modern computing power. 3DES is more powerful than DES due to the three different keys, which is secure as its effective key length is 168 bits, but with two keys effective key length reduces to 112 bits which is less secure [21]. 3DES takes three times CPU power than DES which lowers its performance. AES outperforms 3DES in both in software and hardware. It uses 128-bit fixed length blocks and works with 128,192 and 256 bit keys. It shows the superiority of AES over DES and 3DES [21].

According to different studies on encryption algorithms found that AES algorithms needs less encryption time than RSA consumes the longest encryption time. Also decryption of AES algorithms is better than other algorithms. Using simulation results is evaluated that AES is much better than DES and RSA [22].

According to the comparative analysis of AES and DES security algorithms and found that different machines take different times for encryption/decryption of same algorithms over same data packet. Results showed that AES more secure as compare to DES [25].

Different simulation experiments shows that Blowfish has better performance than other commonly used encryption algorithms. Because of the more processing power AES showed poor performance compared to other algorithms. It shows also that AES consumes more resources when data block size is relatively big. In addition, the experiments proved that 3DES requires always more time than

DES because of its triple phase encryption characteristic. DES and 3DES are known to have worm holes in their security system. Blowfish and AES do not have any worm hole so far [26].

On the basis of detailed study of different symmetric key block ciphers discussed above, an attempt is made to critically analyzes them. DES is one of the encryption algorithms with some weak points. It uses same algorithm for encryption and decryption but the order of the keys is reversed in latter process. With rapid increase in processing speed of CPU and other advances in computing the key space of 56 bit key is considered no more secure from brute force attack.[26]

Algorithm type	Key size	Speed	Block size	Security level
DES	56 Bits	Slow, but speed depends on key	64 bits	Less secure
3DES	112/168 Bits	Very slow	64 bits	Moderately security
AES	128,192,256 Bits	Fast, but speed depends on key	128 bits	Secure
Blowfish	32 – 448 Bits	Fast	64 bits	Believed to be most secured
RSA	1024 Bits - and more	Fast, but speed depends on key	86 bytes	Secure

Figure 4. Comparison of some cryptography algorithms

CONCLUSION

In this paper, we have analyzed DES, 3DES, AES, Blowfish and RSA encryption algorithms. We have found that each algorithm has its own benefits according to different parameters. From the work completed in this paper it is observed that that the strength of the each encryption algorithm depends upon the key management, type of cryptography, number of keys, number of bits used in a key. Longer the key length and data length more will be the power consumption. For security view it is recommended to use short data sequence and key lengths. Since Blowfish has not any known security weak points so far, this makes it an excellent encryption algorithm to be considered as a standard encryption algorithm. AES showed poor performance results compared to other algorithms since it requires more processing power.

According required implementation memory DES and AES require medium size of memory. Also, Blowfish has smallest memory size. RSA consumes more time for encryption and decryption compared to others. Blowfish consumes the least time than other above described algorithms. Blowfish is efficient in software, at least on some software platforms. Evaluating DES, 3DES, AES, Blowfish and RSA we can conclude that Blowfish is strongest against guessing attacks. According different literature survey AES requires highest number of bits to be encoded optimally an encrypted data and DES requires least number of bits to be encoded optimally. Evaluating by time and memory Blowfish is the best than others. According cryptographic strength AES is the strongest algorithm.

The present study provides critical evaluation of these algorithms. For future work can be done comparative or performance analysis with their different parameters to outline the strengths and weaknesses of various algorithms. Nowadays hybrid encryption scheme (symmetric + asymmetric) can have more security level and can ensure more strength, against of any third party attacks.

REFERENCES

1. Applied Cryptography, Second Edition: Protocols, Algorthms, and Source. Bruce Schneier, ISBN: 0471128457, 01.01.1996
2. Introduction to Cryptography, Second Edition, Johhanes A. Buhman, 2000
3. An Introduction to Modern Cryptosystems, Andrew Zwicke, 2003
4. Physical Security of Cryptographic Algorithm Implementations, Ilya KIZHVATOV, L’UNIVERSITÉ DU LUXEMBOURG, 2009
5. Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanston, Massachusetts Institute of Technology, June 1996
6. Diffie, Whitfield; Hellman, Martin (November 1976). "New Directions in Cryptography" (PDF). IEEE Transactions on Information Theory.
7. Cryptographic algorithms and reconfigurable hardware, A Brief Introduction to Modern Cryptography, F. Rodriguez-Henriquez, Diaz Perez, 2007
8. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С, 2-е изд . – М.: Вильямс, 2003.
9. Введение в криптографию, Под редакцией В. В. Ященко, Издание четвертое, 2012
10. Основы криптологии, Д. Ананичева, И. Кориакова, 2006
11. КРИПТОАНАЛИЗ КЛАССИЧЕСКИХ ШИФРОВ, О. Н. ЖДАНОВ, И. А. КУДЕНКОВА , 2008
12. Баричев С. В. Криптография без секретов. – М.: Наука, 1998.
13. A. Sterbenz and P. Lipp, “Performance of the {AES} Candidate Algorithms in {Java},” Third {Advanced Encryption Stand. Candidate Conf. April 13--14, 2000, New York, NY, USA, pp. 161–168, 2000.
14. D. Coppersmith, "The data encryption standard (DES) and its strength against attacks", IBM Journal, Research Develop., vol. 38, no. 3, (1994), pp. 243 -250.
15. Introduction to Modern Cryptography by Phillip Rogaway and Mihir Bellare, 2005
16. D. Elminaam, “Performance evaluation of symmetric encryption algorithms,” Int. J. Comput. Networks, vol. 8, no. 12, pp. 280–286,2008.
17. Ростовцев А. Г., Михайлова Н. В. Методы криптоанализа классических шифров . – М.: Наука, 1995.
18. Криптология – наука о тайнописи //Компьютерное обозрение. –1999.
19. Мао В. Современная криптография: Теория и практика — М.: Вильямс, 2005
20. Ященко В. В. Введение в криптографию. СПб.: Питер, 2001.

21. Hamdan O. Alanazi, B. B. Zaidan, A. A. Zaidan, Hamid A. Jalab, M. Shabbir and Y. Al-Nabhani, “New Comparative Study Between DES, 3DES and AES within Nine factors”, Journal of Computing, Volume, 2, Issue 3, March 2010, pp. 152-157.
22. Dr. Prerna Mahajan and Abhishek Sachdeva, “ A study of Encryption Algorithms AES, DES and RSA for Security”, Global Journal of Computer Science and Technology Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013, pp. 15-22.
23. Deepak Kumar Dakate and Pawan Dubey, “Performance comparison of Symmetric Data Encryption Techniques”, International Journal of Advanced Research in Computer Engineering and Technology, Volume 3, No. 8, August 2012, pp. 163-166.
24. Abdel-Karim Al Tamimi, “Performance Analysis of Data Encryption Algorithms.”
25. Sumitra, “Comparative Analysis of AES and DES security Algorithms”, International Journal of Scientific and Research Publications, Volume 3, Issue 1, January 2013, pp. 1-5.
26. Ayushi, 2010,A Symmetric Key Cryptographic Algorithm, International Journal of Computer Applications (0975 - 8887) Volume 1. No. 15, 2010
27. "Quantum cryptography: An emerging technology in network security". - Sharbaf, M.S. IEEE International Conference on Technologies for Homeland Security . 2011
28. The official Advanced Encryption Standard" (PDF). Computer Security Resource Center. National Institute of Standards and Technology. Retrieved 26 March 2015.
29. "The Digital Millennium Copyright Act of 1998" (PDF). United States Copyright Office. Retrieved 26 March 2015.