Symmetric Key Size for Different Level of Information Classification

SUBARIAH IBRAHIM[1] MOHD AIZAINI MAAROF[2]
Department of Communication and Computer System
Faculty of Computer Science and Information System
Universiti Teknologi Malaysia, Skudai 81310, Johore,
MALAYSIA
[1]Tel: +60-07–557-6160 x 32386, Fax: +60-07–556-5044, E-mail: subariah@fsksm.utm.my
[2]Tel: +60-07–557-6160 x 32009, Fax: +60-07–556-5044, E-mail: maarofma@fsksm.utm.my

Abstract

Information is an important asset to an organization as well as to a nation. Incorrect handling of information may cause economic damage to an organization or cause harm to national security. Some of the information is confidential or sensitive. Confidential information can be categorized into various levels of classification. The classification depends on the level of damage to an organization or to national security when the information is disclosed. Therefore confidential information is normally protected by using cryptographic algorithms. In these algorithms, key is an important element since it is one of the parameters that determine the level of security that the algorithms can provide. The larger the key size, the better security it can provide. Small key sizes are vulnerable to exhaustive attacks. Debates on key sizes were discussed in many literature and documents of software vendors that provide cryptographic solutions. Hence we think that different information classification should be protected with different key sizes. The aim of this paper is to propose key sizes for different classification of information. First we discussed about different levels of information classification. Then we proposed a model to determine adequate key sizes based on Lenstra's model. Our proposed model includes a lifespan of information to be encrypted. By using this model, we then propose key sizes for different levels of information classification.

1. Introduction

Information is an important asset to an organization as well as to a nation. Incorrect handling of information may cause economic damage to an organization or cause harm to national security. In the context of today's open communicating environments, the need for protecting information takes an added importance and significance. Therefore every organization or nation has its own set of requirements for the protection of their information assets, which are usually documented through an information classification policy [1]. The safeguards of information will differ depending on whether the confidentiality, integrity, non-repudiation or availability is being considered. Information which are sensitive can only be disseminated to those who "need to know" that information. This requires a technique for protecting the information while it is stored, used or transmitted. The most established mechanism to protect sensitive information is cryptography.

Cryptographic algorithms are designed to meet certain security objectives such as confidentiality, integrity, authentication and non-repudiation. The security level determines quantitatively to what extent these objectives should be met, for example how long one wants to keep an information in a confidential state. One of the parameters that determine the security level of a cryptographic algorithm is the size of a key. The larger the key size the more secure the cryptosystem against exhaustive key or brute force attack. The difficulty of exhaustive key attack grows exponentially with the number of bits used [2]. Therefore an adequate key size should be used to encrypt information in order to thwart against this attack.

The aim of this paper is to recommend the symmetric ciphers key size for protecting different level of information classification. Lenstra key size determination model states the adequate key size for a particular year [2][3]. However information has different lifespan and a key size should be selected somewhat larger than the lifespan of the protected information [4]. Further, the same cipher will be used to encrypt information in years or decades to come. In this work we enhance Lenstra's model to include a lifespan. From this enhanced model, we then proposed the key sizes for different classification level of information.

In this paper, we first define information classification and review some related work in determining a key size. This review is presented in section 2. We then proposed a key size determination model which is the enhancement of Lenstra's model [4]. We then propose key sizes for different level of information classification. The proposals and some results derived from these models are discussed in section 3. Finally, section 4 concludes the paper.

2. Related Work

Public domain cryptographic algorithms are normally used by commercial organization and hardly used by government to protect government classified information. However in 2003, the Committee on National Security System (CNSS) of United States of America (USA) has designated Advanced Encryption Standard (AES) [5] as suitable for use for classified information [6]. CNSS published a policy fact sheet approving all key lengths of AES as sufficient to protect classified information up to the Secret level while either AES-192 or AES-256 is required for Top Secret information. This is highly significant since Data Encryption Standard (DES) [7] was only rated as suitable for "unclassified" information. This shows that the USA government believes that the public accessed algorithm has a strong security and therefore can be considered to secure Top Secret information. In order to determine the adequate key size for different level of information classification, first we review the definition of information classification and study the key size determination model.

2.1. Information Classification

Information classification is a technique to assign a level of sensitivity to information as it is being created, amended, enhanced, stored or transmitted. This classification determines the extent to which information needs to be controlled or secured and should be based on its potential damage to organization, state, nation or globally if disclosed to unauthorized people [8]. Commercial organizations protect information that gives them an advantage over competitors while governments protect information that gives them an advantage over adversaries. Commercial organizations protect proprietary information such as trade secrets, investment strategies and project plans [9] while nations protect information whose unauthorized disclosure could damage the national security such as military plans, foreign government information and intelligence activities [10]. The objective of classification is not to prevent an adversary from obtaining the information by independent efforts or reverse engineering but rather to avoid assisting the adversary in acquiring that information [11].

2.1.1. Information Classification Definition. Both commercial organizations and governments of nations classify their sensitive information. ISO 17799 classifies information as Top Secret, Highly Confidential, Proprietary, Internal Use Only and Public Documents. The definition of this classification is as follows [9]:

i. Top Secret – Highly sensitive internal documents and data. The distribution is restricted and must be protected at all times. Security is highest possible.
ii. Highly Confidential – Critical information to the organization's ongoing operations and could seriously impede or disrupt them if made shared internally or made public. Security level is very high.
iii. Proprietary – Define the way an organization operates and should be used by authorized personnel only. Security level is high.
iv. Internal use Only – Information not approved for general circulation outside the organization. Security level is controlled but normal.
v. Information approved for public use or distribution. Security level is minimal.

Most governments including USA and Malaysia categorized sensitive information as Top Secret, Secret and Confidential. Some governments such as Australia and New Zealand have an extra classification known as Restricted. The definition for government information classification is as follows [10][12]:

i. Top Secret – The unauthorized disclosure of information could be expected to cause **exceptionally grave damage** to the national security.
ii. Secret – Unauthorized disclosure of information could be expected to cause **serious damage** to the national security.
iii. Confidential – The unauthorized disclosure of information could be expected to cause **damage** to the national security.
iv. Restricted – Information is not for general dissemination. It is often used for controlling the release of reports and other documents until it can be done officially.

2.2. Key Size Determination

The arguments about key size were discussed in many literature and documents of software vendors that provide cryptographic solutions [2][3][13-16]. In 1996 an ad hoc committee reported that technology available in late 1995 were both fast and cheap to make brute force attacks against cryptographic systems that were considered adequate several years before. The report recommended that the key size should be at least 75 bits long to protect information at that time against the most serious threats , that is threats from well-funded commercial enterprises or government intelligence agencies. The report also suggested that 90 bits was the minimum key length needed to provide data security for the next 20 years from late 1995. The recommendation was based on the cost of attack effort [2]. ECRYPT commented that the approach is still reasonably accurate [4]

Lenstra published the first formal work to model key size determination for adequate security [3]. This model formulates a set of hypothesis as a guideline for selecting adequate key size for practical security [3][15]. The hypothesis is as follows:

Hypothesis 1: 56 bit keys were believed to provide adequate security in year 1982.

Hypothesis 2: Every 18 months the amount of computing power and random access memory one gets for a given cost doubles.

Hypothesis 3: The budgets for breaking cryptographic keys doubles every 10 years.

Hypothesis 4: For all systems, the assumption is that no substantial cryptanalytic development will take place.

Hypothesis 2 was based on Moore's Law, which was formulated in 1965 [3][15][16]. According to hypothesis 1 – 4, the adequate key size, K needed in year y will be,

$$K = 56 + 2(y\text{-}1982) / 3 + (y\text{-}1982) / 10. \qquad (1)$$

In 2004, Lenstra updated the model by not taking hypothesis 3 into account. Thereby, adequate protection for year y is calculated as,

$$K = 56 + 2(y\text{-}1982) / 3. \qquad (2)$$

3. Key Size Based on Information Classification

In this section we will discuss the need for different key sizes for different information classification. First the security risks of different class of information are assessed. Then keys size determination model is presented. Finally we recommend the key sizes for different information classification based on the determination model.

3.1. Assessing Security Risks

Classification level is usually determined by the information disclosure risks because those risks largely determine the magnitude of the damage that could be caused by such disclosure [11]. In this section, we will assess the security risks faced by commercial organizations and countries if their sensitive information is disclosed. The objective is to determine whether the damage caused by information disclosure to commercial organizations is similar to a country. This is done by identifying the risks of disclosure of commercial information (CI) and National Security Information (NSI). Table 1 lists some examples of the impacts caused by sensitive information disclosure.

Table 1: Examples of risks for CI and NDI

Type of Organization	Examples of Risks
CI	Loss of reputation
	Loss of customers
	Loss of trade secrets or intellectual property
	Financial loss
	Sabotage
	Bad economic impact to the organization
NSI	Loss of intellectual property
	Loss of life (key government person or public)
	Loss of public safety
	Terrorism
	Jeopardize military security
	Weaken a nation's position in international discussion
	Damage relations with another nation
	Major political damage
	Bad economic impact to the nation
	Social hardship

By examining the risks for both types of organization, we can make an assumption that NSI is more vulnerable than CI. For example a financial loss to CI will only affect a certain number of people or a portion of a nation's population. However a bad economic impact to a nation will affect the whole population thus giving a social hardship to the whole country. Military plan or operation disclosure may risks to military disadvantage to a nation which may affect its sovereignty, hence affecting the whole country. Furthermore, an organization or country is willing to spend more money to damage a country then a commercial organization. Therefore we can say that disclosure of NSI is more vulnerable than the disclosure of CI.

Based on the above discussion, we recommend that key sizes for NSI should be longer then the one used in CI. For NSI, classification level indicates the relative importance of classified information to national security. According to [11], the distinction between Secret and Top Secret information appears to be that Top Secret information is “vital”, whereas Secret information is only “significant”. The author also stated that Secret documents gave the entire description of a process or of key equipment, etc. whereas Confidential documents revealed only fragmentary information i.e. not the critical information. Therefore we also recommend that different classification level of NSI should use different key size with higher classification or more sensitive information using longer size. This is aligned with US government policy which allows the use of AES-128 for Confidential and Secret while AES-192 or AES-256 for Top Secret classified information [6].

3.2. Modified Key Size Determination Model

In Lenstra’s model, he uses an assumption that DES offered a sufficient protection for commercial application. If we take Blaze *et al.*’s recommendation that 75 bits is adequate in late 1995 [2], then equation (2) can be modified to,

$$K = 75 + 2(y- 1995) / 3. \qquad (3)$$

Lenstra stipulated that if one feels that DES can still be trusted in year y_a, then 1982 can be replaced by y_a. Thus by considering different key size k_a is adequate for different year y_a, equation (2) can be modified to a more general formula as follows:

$$K = k_a + 2(y- y_a) / 3. \qquad (4)$$

Therefore Lenstra’s hypothesis 1 can be made more generalized as follows:

Hypothesis 1: Key size k_a is adequate for year y_a.

3.2.1. Modified Model with Lifespan. There is a wide variety of digital information with varying economic values and privacy aspects as well as a wide variation in the time over which the information needs to be protected. A trade secret has high economic value, government classifies information according to different levels of access and confidentiality as well as how detrimental it is to the national security. These varieties of information have different lifespan that is the period in which it is functional. Some of the information requires to be kept confidential with various life times. For example, electronic fund transfer has a short term security with a lifespan that lasts in just a few minutes; a proprietary product has a lifespan of several decades while individual private information may be kept confidential during his lifetime. [2][17].

As different information has different lifespan, we proposed that a lifespan, *ls* is included in the model. Since Lenstra’s hypothesis 3 is not considered, the hypothesis is replaced with the following hypothesis:

Hypothesis 3: The confidentiality of different information has various lifespan.

Thus a key size is calculated as,

$$K = k_a + 2(y + ls - y_a) / 3 \qquad (5)$$

Using equation (5), we calculate the key sizes needed for various lifespan taking into account when the information will be encrypted. We compute from year 2005 until 2030 with five year increment for the year information will be encrypted. This is to show if the same algorithm is still being used in 2030 as in 2005, we need to consider that information may be decrypted some years later and therefore the key size need to be catered at the end of that information’s lifespan. We calculated the adequate key sizes by using Lenstra’s recommendation for hypothesis 1. The results are as shown in Table 2. The key sizes in the tables are round-up to a whole number. The key size calculation shows that AES-128 is still adequate until 2030 with 25 years lifespan information.

Table 2: Adequate key size with lifespan

Year Encrypt	Lifespan in Years					
	1	5	10	15	20	25
2005	72	75	78	81	85	88
2010	75	78	81	85	88	91
2015	79	81	85	88	91	95
2020	82	85	88	91	95	98
2025	85	88	91	95	98	101
2030	89	91	95	98	101	105

3.3. Key Size Model for Information Classification

As discussed in section 3.1, we recommend that NSI should use a longer key than CI. We also recommended that different level of NSI should use different key sizes with more sensitive information using a longer key. Thus we need to define levels of information as shown in Table 3.

Table 3: Information levels

Level	Type of Information
0	Commercial Information
1	Confidential Classified Information
2	Secret Classified Information
3	Top Secret Classified Information

Based on the above conclusion, we proposed an equation for calculating adequate key size for different level of information as follows:

$$K = k_a + 2(y + ls - y_a) / 3 + l*K_{inc} \qquad (6)$$

Where l is the information level and K_{inc} is the difference of key sizes offered by an algorithm with variable key sizes. Most algorithms offer a fixed increment, for example AES has a key increment of 64 bits. The increment is normally in powers of 2, for example 16 bits, 32 bits and 64 bits. In order to identify the best choice K_{inc}, we compare the key sizes obtained by using K_{inc} = 16, 32 and 64 bits with the one used by USA government [6]. Tables 4-7 gives the key sizes for different information classification level when different key increment is used for some encryption years and lifespan. The key sizes used by USA government are also shown in the table for comparison purposes.

Table 4: Key sizes for year 2005 and lifespan = 1 year

Type of Information	USA Policy on Key Size	K_{inc}		
		16-bit	32-bit	64-bit
Commercial	128	72	72	72
Confidential	128	88	104	136
Secret	128	104	136	200
Top Secret	196	120	168	264

Table 5: Key sizes for year 2005 and lifespan = 25 years

Type of Information	USA Policy on Key Size	K_{inc}		
		16-bit	32-bit	64-bit
Commercial	128	88	88	88
Confidential	128	104	120	152
Secret	128	120	152	216
Top Secret	196	136	184	280

Table 6: Key sizes for year 2030 and lifespan = 1 year

Type of Information	USA Policy on Key Size	K_{inc}		
		16-bit	32-bit	64-bit
Commercial	128	89	89	89
Confidential	128	105	121	153
Secret	128	121	153	217
Top Secret	196	137	185	281

Table 7: Key sizes for year 2030 and lifespan = 25 years

Type of Information	USA Policy on Key Size	K_{inc}		
		16-bit	32-bit	64-bit
Commercial	128	105	105	105
Confidential	128	121	137	169
Secret	128	137	169	233
Top Secret	196	153	201	297

The tables show that key sizes with 16-bit increment are too small for Top Secret information and key sizes with 64-bit increment are too high for all classes of NSI when compared to the key sizes recommended for USA Government NSI. Key sizes with 32-bit increment seems to be more aligned to USA government policy on key size when compared to the other two increments since only the Secret information has a higher key size. This is because the USA government allows both Confidential and Secret information to use the same key size. However in our opinion, both of these information types should use different key sizes since their risks are different. Therefore we recommend that adequate key sizes for different levels of classified information for various years of encryption and lifespan can be obtained by using equation (6) with K_{inc}.= 32-bit. The adequate key size for commercial application is similar to Table 2. The key sizes for different levels of information for NSI can be obtained by using equation (6).

4. Conclusion

Since USA government trusts that public accessed cryptographic algorithm can be used to protect classified information up to Top Secret level, we therefore study the key size determination model for different classification of information. Our work is based on Lenstra's key size model. We then enhanced his model to include a lifespan since the confidentiality of information has various periods. To determine the key size for different classification we add two more parameters which are classification level and key size increment to our enhanced model.

Our model shows that the key size for classified information is aligned with the one recommended by CNSS of USA. Therefore we recommend our model to be used as a guideline for determining a key size range when designing a scalable cipher which can be used to protect public information as well as classified government information. It is important to note that long key size alone does not guarantee the strength of a cryptographic algorithm. Other factors such as the quality of implementation of the algorithm in specific software, firmware or hardware and key management activities also play a role in determining the strength of the algorithm.

Acknowledgements

The authors would like thank UTM and MOSTI for their financial support in this work.

References

[1] Peltier, T.R., Information Security Risk Analysis, Auerbach Publication, Boca Raton, Florida, 2001.

[2] Blaze, M., Diffie, W., Rivest, W., Schneier, B., Shimomuro, T., Thompson, E. and Wiener, M., Minimal Key lengths for Symmetric Ciphers to Provide Adequate Commercial Security. *A Report by an Ad Hoc Group of Cryptographers and Computer Scientist*, 1996.

[3] Lenstra, A.K. and Verheul, E.R., Selecting Cryptographic Key Sizes. *Journal of Cryptology*, 14(4), 2000, pp. 255-293.

[4] ECRYPT, ECRYPT Yearly Report on Algorithms and Keysizes, IST-2001-507932, 2004.

[5] *FIPS 197*. Specifications for the Advanced Encryption Standard (AES). National Institute of Standards and Technology, U.S. Department of Commerce, Washington D.C., 2001.

[6] CNSS Policy No. 15, National Policy on the Use of the AES to Protect National Security Systems and National Security Information, June, 2003.

[7] FIPS 46-2, *Data Encryption Standard*. Federal Information Processing Standard (FIPS), Publication 46-2, National Institute of Standards and Technology, U.S. Department of Commerce, Washington D.C., 1993.

[8] Data Classification, http://www.yourwindow.to/information-security/gl_dataclassification.

[9] ISO 17799 News, Establishing Information Classification Criteria, Issue 9.

[10] EO 12958, Classified National Security Information, The White House, April 17, 1995.

[11] Quist, A.S., Security Classification of Information, Vol. 2: Principles for Classification of Information, Oak Ridge National Laboratory, Tennessee, USA.

[12] Classified Definition. http://www.answers.com/topic/classified-information

[13] Stallings, W., *Cryptography and Network Security: Principles and Practices*, 3rd Edition. Upper Saddle River, New Jersey: Prentice Hall, 2003.

[14] Canda, V., Trung, T.V., Magliveras, S. and Horvath, T., Symmetric Block Ciphers Based on Group Bases. *SAC 2000, LNCS 2012*, Springer-Verlag, 2001, pp. 89-105.

[15] Fibikova, L. and Vyskoc, J., Practical Cryptography – the Key Size Problem: PGP After Years. *Proceedings in Workshop "Santa's Get Together"*, December 10-11, 2001, Prague.

[16] Preneel, B., Cryptographic Challenges: The Past and the Future, A.E. Abdallah, P.Ryan and S. Svhmeider (Eds.), *FASec 2002, LNCS 2629*, Springer-Verlag, 2003, pp. 167-182.

[17] Schneier, B. and Kelsey, J., Unbalanced Feistel Networks and Block Cipher Design. *In Proceedings of Fast Software Encryption 1996.* Springer-Verlag, 1996, pp. 121-144.