International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 12, December-2014

Performance Analysis of the Encryption Approach used by the Portuguese E-Procurement

Ricardo Garcês
Academia de Informática Brava-Engenharia de Sistemas Lda
Rua 1º de Julho
9350-206 Ribeira Brava – Madeira, Portugal

Fernando Morgado-Dias
Madeira Interactive Technologies Institute and Centro de Competências de Ciências Exactas e da Engenharia, Universidade da Madeira Campus da Penteada, 9000-039 Funchal, Madeira, Portugal.

***Abstract*— The Portuguese e-procurement platforms are obliged to provide mechanisms based on asymmetric encryption in order to safeguard the confidentiality and integrity of the proposals submitted by the bidders. However, asymmetric encryption was designed to encrypt small data blocks. This can be a major challenge to the performance provided by the e-procurement platforms. In fact, the documents submitted by the bidders may in many cases reach to hundreds of megabytes. Therefore, these mechanisms must be able to encrypt large documents in a feasible amount of time. Because the performance provided by the encryption mechanisms is a key factor in the success of an e-procurement platform, this article evaluates two different encryption models in order to determine the one that provides the best performance. During the analysis of the e-procurement encryption process we were able to verify that the exclusive use of asymmetric encryption by the Portuguese e-procurement platforms is not feasible. In fact, it is not feasible that a bidder would need to wait almost a day to encrypt a single document with only 500 000 kb. It is also not feasible that the authorized entities would have to wait more than one day to decrypt the same document.**

Keywords*— *E-procurement, symmetric encryption, asymmetric encryption, hybrid approach, performance.

I. INTRODUCTION

According to [7], Portugal is one of the leading European countries in the public e-procurement area. In fact, the vast majority of the Portuguese public contracts are awarded using e-procurement platforms. These platforms are managed by private entities and there are seven companies authorized to offer this service [8]. The Portuguese public sector is obliged to acquire the services of one of these entities, in order to award their contracts. However, the registration and use of these platforms by the bidders is free of costs.

The several transactions, required by law, related with a procurement procedure are based on the use of electronic means. In fact, as displayed in figure 1, all communications and exchange of information between the bidders and the contracting entities related with a procurement procedure are made through the e-procurement platforms.

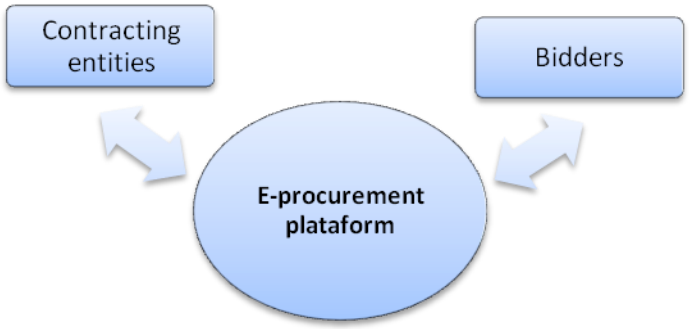

Figure 1: The Functioning of An E-Procurement Platform

According to [16], the security and authentication are a key factor to the success of an e-procurement project. Therefore, the e-procurement platforms must be compliant with the technological requirements defined by the Portuguese legislation regarding the authenticity, integrity and confidentiality of the data loaded.

On a public procurement procedure, all the documents and information included in the proposals, applications or solutions, submitted by the several bidders, should only be consulted by the authorized entities after the end of the legally established deadline. In fact, it would be a very serious security failure that a competitor, or other entity, could have access to the information contained in the proposals, applications or solutions before the end of the deadline set for its submission.

In order to safeguard these situations, the Portuguese Ordinance 701-G/2008 states that all documents that make up the proposals, applications or solutions, loaded to the e-procurement platforms should be encrypted using asymmetric cryptography based on the use of key exchange.

However according to [9], asymmetric encryption has an important limitation in terms of performance. It is computationally burdensome and inefficient when trying to encrypt data blocks with some dimension.

The performance of the e-procurement platforms is a key factor on its acceptance by all the involved parties. In fact, it is crucial that the encryption schema used by the e-procurement platforms, provides the best performance possible on the encryption/decryption of the data, without neglecting its security guaranties. This could constitute a major obstacle in the exclusive use of the asymmetric encryption model as proposed by the Ordinance 701-G/2008.

As an alternative to the exclusive use of the asymmetric encryption model, a hybrid approach is widely used to encrypt large files while keeping the security guaranties of the asymmetric encryption schema.

This paper evaluates the performance of asymmetric encryption algorithms as opposed to symmetric algorithms used by the hybrid encryption approach. The time allocated to encrypt/decrypt different sizes of data blocks with each one of these algorithms will be compared. This analysis will allow us to determine the encryption model and algorithms that provide the best performance in the encryption of large files by the Portuguese e-procurement platforms.

A. *Related Work*

There are usually two approaches used worldwide to ensure the security of the bid submission process [5]. One based on a Public Key Infrastructure and the other based on the use of the user id and password to secure and encrypt information.

The Indian e-procurement framework is based on a Public Key Infrastructure bid-encryption. In [3] the guidelines of the quality requirement for the Indian e-procurement platforms are detailed, and concerns related with the use of a Public Key Infrastructure based Bid-Encryption are addressed. It also states that public key algorithms are slow. This is a crucial aspect that has to be addressed by the e-procurement platforms. In fact, according to [16] security and authentication on the e-procurement infrastructures is a key factor for the success of a public e-procurement project, however, performance plays also a key role on its success.

The European Commission defined the functional guideline for conducting public e-procurement procedures [6]. These guidelines address to security issues stating that the stored data should be encrypted using proven secure symmetric algorithms.

B. *Asymmetric encryption*

Asymmetric encryption is based on the Diffie-Hellman Key Exchange [4]. According to this algorithm, each user is assigned a pair of keys: a public key, which will be available to all the interested parties, and a private key that is to be kept secret. Data encryption is performed using the public key by anyone who has access to it, however, the decryption of the data can only be made by those who hold the private key, as can be seen in figure 2.

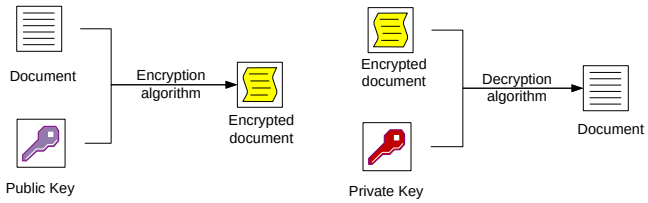

Figure 2: Asymmetric encryption

The Ordinance 701-G/2008 specifies that asymmetric cryptography should be used for encryption of uploaded documents by the bidders. It is mandatory that the Portuguese e-procurement platforms issue a digital certificate (containing a public and private key pair) for each procurement procedure.

The public key will be used in the encryption of the documents submitted by the bidders. Therefore it should be available to the bidders in order that they could be able to encrypt the data and documents that make up their proposals, applications or solutions.

On the other hand, the Portuguese legislation defines that the e-procurement platforms should be responsible for the custody of the private key and should only provide access to it after the end of the deadline for the proposals, applications or solutions submission, allowing that the encrypted information can be decrypted.

Asymmetric encryption algorithms are designed to encrypt data blocks smaller than its public key size minus a variable number of bytes of overhead. For example, with a 2048-bit key we should only be able to encrypt a data block up to 245 bytes (256 bytes of the public key size minus 11 bytes of overhead). However, the documents submitted by the bidders, can in many cases, easily reach to hundreds of megabytes. Therefore we would be forced to split the documents into very small chucks and then encrypt them. This process will result in a set of encrypted data blocks with a total size significantly bigger than the size of the original file. According to [9] this encryption schema would also require a significant consumption of time and computer processing resources.

C. *Symmetric encryption*

As opposed to asymmetric cryptography appears symmetric encryption. According to [15], one of the major advantages of the symmetric encryption model is the speed and efficiency of its algorithms. They can reach speeds of encryption/decryption hundreds or even thousands of times faster than asymmetric algorithms.

According to [4], in the symmetric encryption model both the sender and the receiver have a common key, used for encoding information. This common key would also be used to decode the encrypted information, as can be seen in figure 3.

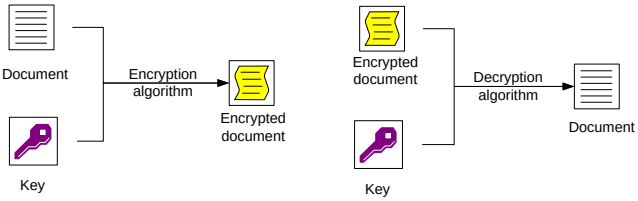

Figure 3: Symmetric encryption

However, the exclusive use of the symmetric cryptography model in order to encrypt the uploaded documents by the bidder of an e-procurement procedure is still not a good solution.

In fact, the electronic platforms users would have access to a common key used to encrypt the documents but also to decrypt the same documents. So there would be no guarantees that someone, with access to documents loaded to the e-procurement platforms, wouldn't have decrypted them before the deadline set for the submission of the bidders proposals.

D. *Hybrid approach*

According to [15], and in order to solve this problem, we should use a hybrid solution based on the union the symmetric and asymmetric models, combining the best aspects of each model.

In this hybrid approach, the data is encrypted using a symmetric algorithm and then the symmetric key used is encrypted by an asymmetric algorithm, as can be seen in figure 4. This approach benefits of the speed of the symmetric encryption but also of the security offered by the asymmetric encryption key distribution method.

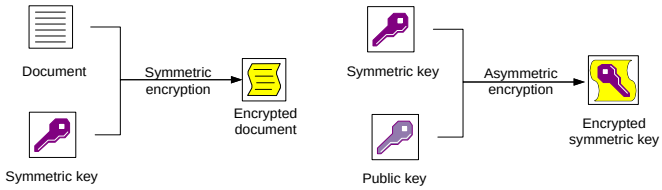

Figure 4: Encryption Using The Hybrid Approach

Using this approach, for each one of the documents loaded by the bidders a symmetric key should be automatically generated. This key should be used to encrypt the loaded document. This key would also be asymmetrically encrypted using the public key of the e-procurement procedure.

The symmetric keys used to encrypt each one of the documents loaded to the e-procurement platforms should be generated and encrypted locally on the bidder's computer and only then transmitted to the e-procurement platforms. This would give us guarantees that only the bidder had access to the unencrypted symmetric keys used to encrypt the documents that make up the proposal.

The decryption of the data would only be possible after the private key of the e-procedure is made available. This private key is needed to decrypt the symmetric keys used to encrypt the documents and data submitted by the bidders, as can be seen in figure 5.

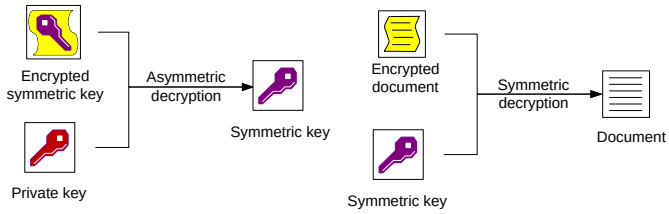

Figure 5: Decryption using the hybrid approach

E. *Symmetric and Asymmetric Encryption algorithms*

Several symmetric and asymmetric encryption algorithms are widely used in information security. However, given the exponential increase of the processing capability of today's computers, it is important to assure that the encryption algorithms used are effectively secure.

The United States National Institute of Standards and Technology defined time periods when different sets of encryption algorithms are considered secure [1]. In the following table the symmetric and asymmetric encryption algorithms (and their minimum key size) considered secure through 2030 are listed.

Table1: Secure encryption algorithms through 2030

Type	Algorithm	Key Size	Description
Symmetric	3DES	192	Triple-Data Encryption Standard (3DES) is a minor variation of Data Encryption Standard (DES) algorithm. Nowadays, the DES algorithm is vulnerable to brute-force attacks. In order to resolve this problem, the 3DES algorithm encrypts data blocks consecutively with 3 keys of 64 bits each. This makes the 3DES algorithm slower than the original DES algorithm. However, it will provide a greater security guaranty [10].
Symmetric	AES	128, 192 and 256	Advanced Encryption Standard (AES) cipher algorithm has been developed to replace DES. This algorithm was adopted as a cryptographic standard by the United States government and is also widely used globally. According to [10], AES has proven to offer a high performance with low resources requirements.
Asymmetric	RSA	2048	RSA (created by Ron Rivest, Adi Shamir, and Leonard Adleman) is the most used public-key encryption algorithm. As stated in [10], this algorithm is based on the factorization of two large prime numbers in order to derivate a set of two numbers that constitutes the public key and another set that is the private key.

The encryption algorithms listed previously will be evaluated, in order to determine the ones that provide the lowest encryption/decryption time using the asymmetric encryption approach and the hybrid approach.

II. Experimental Set-Up Design

In order to collect data about the performance of the encryption algorithms the following setup will be used:

- Laptop with 2.00 GHz C.P.U., 2GB RAM;
- Windows 7 operating system (32-Bit);
- OpenSSL 1.0.1c software (OpenSSL cryptographic library).

In this experiment, there will be encrypted/decrypted text files that range from 50 kb to 500 000 kb with:

- RSA (exclusive use of asymmetric encryption);
- 3DES and AES algorithms (hybrid approach).

The time will be calculated in milliseconds taken by each algorithm to encrypt/decrypt each file according to the approach taken.

For the exclusive use of asymmetric encryption approach the files will be divided into data blocks with a maximum size of 245 bytes (this is the maximum size supported by RSA with a key size of 2048 bytes).

For each encryption algorithm evaluated the average encryption/decryption time in milliseconds for 1 kb will also be calculated.

III. EXPERIMENTAL RESULTS

In the following table is displayed the time consumed in milliseconds by the selected encryption algorithms in order to encrypt text files with different sizes.

Table 2: Encryption experimental results

	Asymmetric encryption	Hybrid approach			
Text File Size (kb)	RSA (2048)	3DES (192)	AES (128)	AES (192)	AES (256)
50	6938	292	212	234	258
100	17142	305	219	236	241
250	40816	320	223	240	244
500	81632	343	226	250	251
1000	167346	386	250	259	266
2500	397959	550	509	302	358
5000	877551	769	513	357	387
10000	1673469	1143	634	536	537
25000	4183673	2878	2200	1128	1010
50000	8775510	6077	4218	2289	5232
100000	16734693	12126	9551	7818	10105
250000	42857142	32595	32456	29939	36848
500000	83673469	69854	51861		61978
Average encryption time (ms/kb)	165,77	0,95	0,68	0,72	0,78

In the following table is displayed the time in milliseconds consumed to decrypt text files with different sizes by the several encryption algorithms.

IV. DISCUSSION

As we can verify in figure 6, the average encryption time consumed to encrypt a kb by the exclusive asymmetric encryption approach takes more than 165 milliseconds while all the algorithms evaluated using the hybrid approach take less than a millisecond.

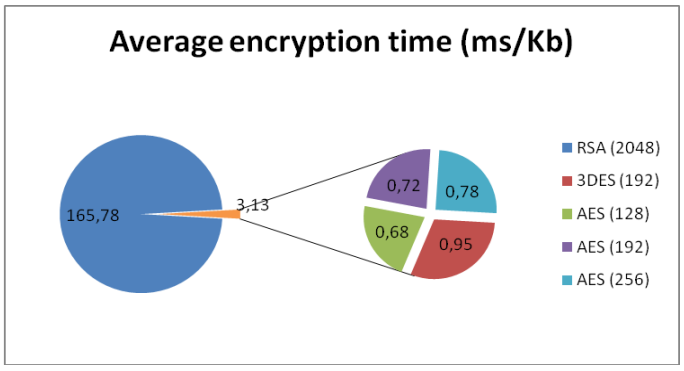

Figure 6: Average encryption time

This abysmal difference in terms of time consuming between both models is also very clear in the average decryption time calculated for all the encryption algorithms evaluated, as we can see in figure 7.

Table 3: Decryption experimental results

	Asymmetric encryption	Hybrid approach			
Text File Size (kb)	RSA (2048)	3DES (192)	AES (128)	AES (192)	AES (256)
50	10612	158	92	104	91
100	22040	153	102	148	161
250	66326	168	122	177	178
500	102040	210	160	170	258
1000	212244	222	273	186	308
2500	510204	461	294	233	619
5000	1122448	600	328	309	1112
10000	2040816	1369	500	456	1448
25000	5510204	2508	1031	2234	2692
50000	11224489	6012	2059	3850	2697
100000	27346938	13082	8413	9614	7749
250000	53061224	33912	35478	31965	29893
500000	114285714	72463	52454	50363	56202
Average decryption time (ms/kb)	223,55	0,54	0,35	0,42	0,47

As stated by [9] the results obtained clearly show that the exclusive asymmetric encryption approach requires significant time consumption to encrypt/decrypt large files. In fact, as we can see in figure 8 the encryption time of a large file with 500 000 kb reaches to almost a day. The decryption type consumed by this encryption model is also high. As showed in figure 9 it would take more than a day to decrypt a file with 500 000 kb.

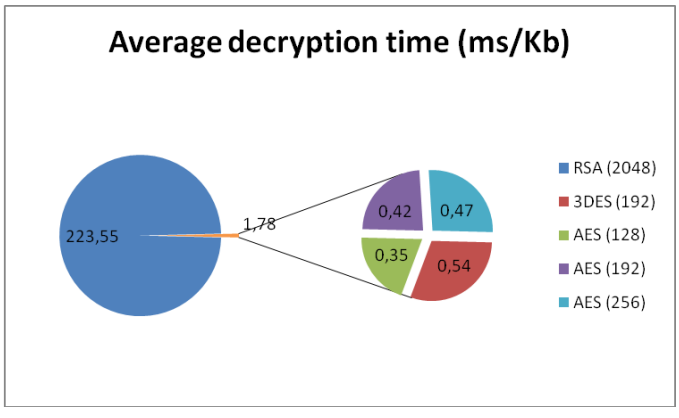

Figure 7: Average decryption time

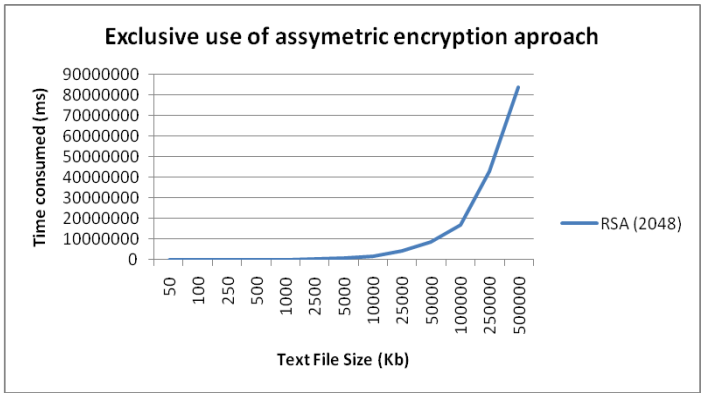

Figure 8: Encryption using the exclusive asymmetric encryption approach

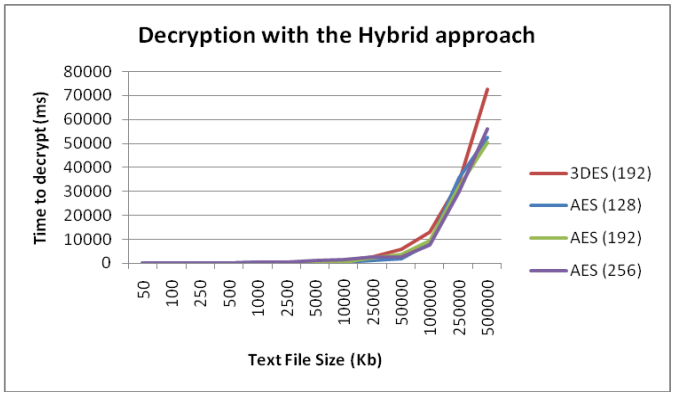

Figure 11: Decryption Using The Hybrid Approach

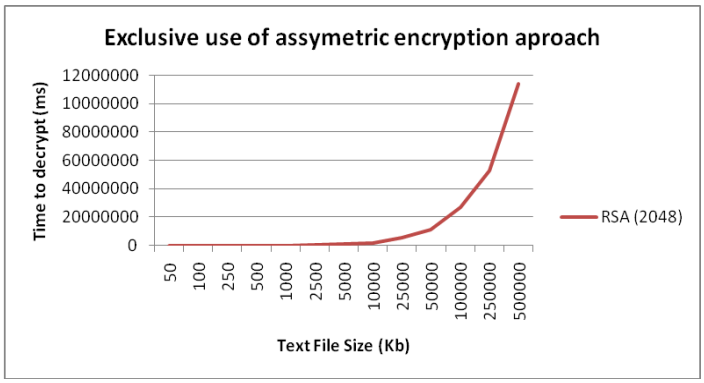

Figure 9: Decryption using the exclusive asymmetric encryption approach

Using the hybrid approach the time consumed to encrypt/decrypt the files has proven to be much smaller when compared with the exclusive asymmetric encryption approach. As showed is figure 10, the symmetric encryption algorithms evaluated take from 0.8 to 1.2 minutes to encrypt a file with 500 000 kb. The time consumed to decrypt this same file by the several encryption algorithms evaluated is also quite low. In fact, it also takes from 0.8 to 1.2 minutes to decrypt a file with 500 000 kb, as we can see in figure 11.

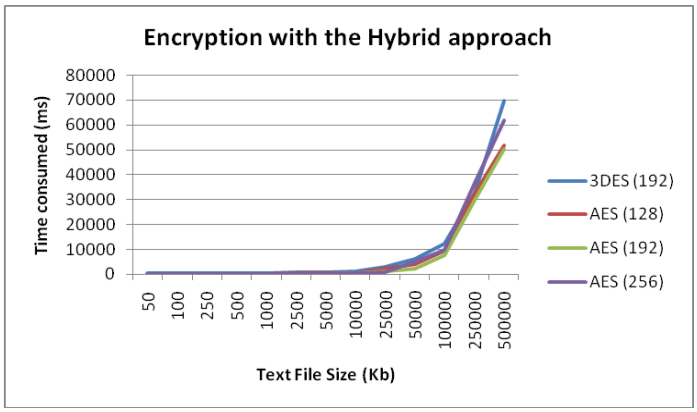

Figure 10: Encryption Using The Hybrid Approach

As showed in the figure 12, within the hybrid approach, the several symmetric encryption algorithms evaluated showed slight differences in terms of performance:

- As expected, the 3DES algorithm has presented a worst performance when compared with the variants of the AES algorithm evaluated.
- The performance of the AES algorithm variants evaluated has proportionally decreased as the size of the key used grew.
- The AES algorithm with a key size of 128 bits provided the best average time of encryption, followed by AES with a key size of 192 bits (6% slower) and AES with a key size of 256 bits (15% slower). The 3DES algorithm offered the worst average time of decryption, 40% slower that the AES algorithm with a key size of 128 bits.
- The AES algorithm with a key size of 128 bits provided the best average time of decryption, followed by AES with a key size of 192 bits (20% slower) and AES with a key size of 256 bits (34% slower). The 3DES offered the worst average time, taking in average more 54% to decrypt 1 kb.

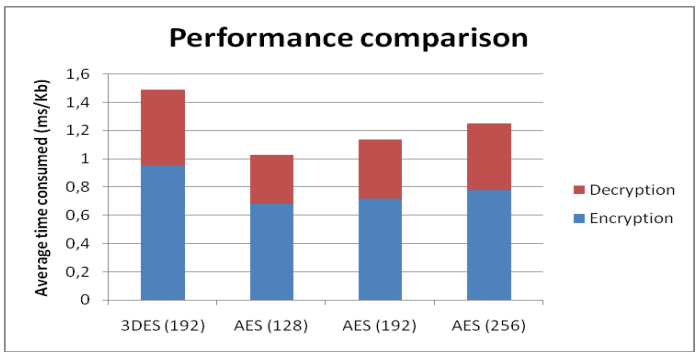

Figure 12: Performance comparison

Combining the average time in milliseconds consumed to encrypt and decrypt 1 kb of data, AES with a key size of 128 bits offers the best time (1,03 ms) followed by AES with a key size of 192 bits (1,14 ms and 11% slower) and AES with a key size of 256 bits (1.25 ms and 21% slower). 3DES with a key size of 192 bits offers the worst time (1.49 ms and 45% slower).

V. CONCLUSIONS

With this analysis it became very clear that the exclusive use of asymmetric encryption as required by the Ordinance 701-G/2008 is not feasible. In fact, It is not feasible that a bidder would need to wait almost a day to encrypt a single document with only 500 000 kb. Is it also not feasible that the authorized entities would have to wait more than one day to decrypt the same document.

This analysis also left no doubt that the hybrid approach offers a much better solution when encrypting large files. Actually according to the data collected, when using the hybrid approach, the bidders would have to wait at most, less that 1.2 minutes to encrypt a file with 500 000 kb. The authorized entities would also have to wait around the same time to decrypt the same file.

Therefore the Ordinance 701-G/2008 should by clarified, declaring that the proposals, applications and solutions submitted by the bidders should be encrypted using a hybrid approach.

This analysis also allowed us to evaluate the performance of 3DES and AES algorithms with key sizes considered secure through 2030. As expected, the 3DES algorithm has proven to clearly have a lower performance when compared to the AES algorithm. Within the several key sizes variants of the AES algorithm evaluated, the difference registered in terms of performance was smaller. However, the key size of 128 bits provided the best performance both encrypting and decryption the information.

REFERENCES

[1] Barker, E., Barker, W., Burr, W., Polk, W., Smid, M., 2007. Computer Security - Recommendation for Key March, 2007 Management – Part 1: General. NIST Special Publication 800-57.

[2] Bovis, C.H., 2007. EU Public Procurement Law. Edward Elgar Publishing Limited.

[3] DEIT, 2011. "Guidelines for compliance to Quality requirements of eProcurement Systems." Department of Electronics and Information Technology. Retrieved 27/03/2013, from http://www.mit.gov.in/sites/upload_files/dit/files/eprocurementdraftguidelines_9112011.pdf.

[4] Delfs, H., Knebl, H., 2007. Introduction to Cryptography: Principles and Applications. Springer, pp. 33-80.

[5] DESA,, 2011. E-Procurement: Towards Transparency and Efficiency in Public Service Delivery. Department of Economic and Social Affairs - Division for Public Administration and Development Management, United Nations Headquarters, New York.

[6] EC, 2005. "Function requirements for conducting eletronic public procurement under the EU framework." European Comission. Retrieved 27/03/2013, from http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/functional-reguirements-vol1_en.pdf.

[7] EC, 2010. "UE Procurement Green Paper." European Comission. Retrieved 27/03/2013, from http://ec.europa.eu/internal_market/consultations/docs/2010/e-procurement/green-paper_pt.pdf.

[8] IBRE, 2013. "Electronic Platforms / Certified entities." BASE: Public contract online, Institute of Building and Real Estate, P.I. Retrieved 27/03/2013, from http://www.base.gov.pt/base2/html/plataformas/plataformascertificadas.shtml.

[9] Martin, K.M., 2012. Everyday Cryptography: Fundamental Principles and Applications. Oxford University Press, pp. 150-185.

[10] Pachghare, V.K., 2009. Cryptography And Information Security. Prentice Hall of India, pp. 32-86, 125-129.

[11] Pani, A.K., Agrahari, A., 2007. E-Procurement in emerging Economies: Theory and Cases. Idea Group Publishing.

[12] PG, 2008. Decree-Law 18/2008. Portuguese Government.

[13] PG, 2008. Ordinance 701-G/2008. Portuguese Government.

[14] Stallings, W., 2003. Cryptography and Network Security - Principles and Practice. Prentice Hall.

[15] Umar, A., 2003. Information Security And Auditing in the Digital Age. NGE Solutions Inc., pp. 4-12.

[16] Vaidya, K., A. S. M., S., Callender, G., 2006. Critical factors that influence e-procurement implementation success in the public sector, Journal of public procurement.