Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 12, December 2019, pg.25 – 33

PERFORMANCE EVALUATION OF CLOUD DATA SECURITY FRAMEWORK USING SYMMETRIC KEY ALGORITHM

Mr. C. PRAKASH
Assistant Professor, Department of Information Technology, Dr. NGP College of Arts & Science, Coimbatore - 48

Abstract: - There exist numerous kinds of cryptographic structures. In symmetric cryptography, both sending and receiving events share the identical secret key. While symmetric cryptography is computationally green, it requires that the shared secret key is sent to all recipients in a comfy way. Public-key cryptography additionally referred to as uneven cryptography, uses two keys: a public key that can be freely shared and a non-public key, which is mathematically tied to the public key. In public-key signature schemes, the creator of the content material makes use of the private key to signal the content. Afterwards the general public key and the signature are disbursed at the side of the content, permitting the recipient to verify the content material's authenticity.
Encryption algorithms play a major role in records security systems. On the alternative side, the ones algorithms eat a massive quantity of computing assets which include CPU time, memory, and battery power. This thesis provides evaluation of six of the maximum not unusual encryption algorithms specifically: AES (Rijndael), DES, and Blowfish.
A comparison has been carried out for the ones encryption algorithms at distinctive settings for each set of rules inclusive of one of kind sizes of information blocks, extraordinary statistics sorts, battery power intake, one of a kind key length and eventually encryption/decryption speed. Simulation results are given to illustrate the effectiveness of every algorithm.
Keywords: - Cryptography, Symmetric Key, DES, AES, Blowfish, Encryption, Decryption.

1. INTRODUCTION

Cryptography has been derived from the Greek phrases: kryptós, "hidden", and gráphein, "to write" - or "hidden writing". People who study and increase cryptography are referred to as cryptographers and the take a look at of cryptography is referred to as cryptanalysis, or code breaking. Cryptography and cryptanalysis are now and again grouped together underneath the umbrella time period cryptology, encompassing the whole situation.

Some cryptographic methods rely upon the secrecy of the algorithms; such algorithms are most effective of historical interest and aren't good enough for real-international needs. All current algorithms use a key to control encryption and decryption; a message can be decrypted only if the important thing matches the encryption key.

There are two instructions of key-based encryption algorithms, symmetric (or secret-key) and uneven (or public-key) algorithms. The distinction is that symmetric algorithms use the same key for encryption and

decryption (or the decryption key is without problems derived from the encryption key), whereas uneven algorithms use a extraordinary key for encryption and decryption, and the decryption key can not be derived from the encryption key (each consumer has a public key and a non-public key; the public secret is made public even as the non-public key remains secret; encryption is carried out with the general public key even as decryption is finished with the private key).

Cryptography plays a totally essential function in retaining the message secure as the facts is in transit. It ensures that the message being dispatched at one stop remains personal and must be acquired simplest via the supposed receiver at the other give up. Cryptography converts the original message in to non readable layout and sends the message over an insecure channel. The folks that are unauthorized to study the message attempt to interrupt the non readable message but it's far hard to do it so. The authorized person has the functionality to convert the non readable message to readable one. The authentic message or the real message that the person wishes to speak with the alternative is described as Plain Text.

The message that can't be understood through everyone or meaningless message is what we call as Cipher Text. Encryption is the manner of changing plaintext into cipher text with a key. A Key is a numeric or alpha numeric text or may be a unique symbol. A decryption is a opposite process of encryption wherein unique message is retrieved from the cipher text. Encryption takes region on the sender stop and Decryption takes place on the receiver stop. Figure 1.1 indicates the encryption/decryption manner of a plaintext message. The enter to the encryption process is plain text and that of decryption method is cipher text. First the plaintext is passed through the encryption set of rules which encrypts the plaintext the use of a key after which the produced cipher text is transmitted.

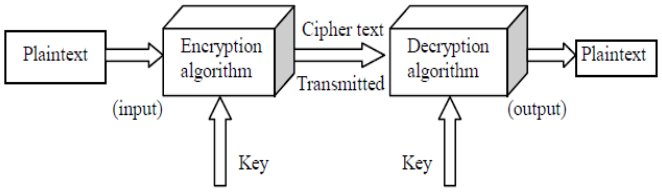

Fig 1.1: - Encryption / Decryption Process

Symmetric algorithms may be divided into circulate ciphers and block ciphers. Stream ciphers can encrypt a single bit of plaintext at a time, while block ciphers take a number of bits (generally 64 bits in contemporary ciphers), and encrypt them as a unmarried unit. Asymmetric ciphers (also known as public-key algorithms or commonly public-key cryptography) permit the encryption key to be public (it could even be published in a newspaper), allowing all people to encrypt with the important thing, whereas handiest the right recipient (who knows the decryption key) can decrypt the message. The encryption key is also known as the general public key and the decryption keys the private key or secret key.

2. CLOUD DATA SECURITY

Cloud computing is a distributed computing fashion which provide integration of net offerings and facts centres. There are numerous fundamental cloud computing vendors such as Amazon, Google, Yahoo, Microsoft and others which can be imparting cloud computing offerings. Amazon net services changed into first to provide an architecture for cloud primarily based offerings in 2002 and after that improvements and new fashions for cloud architecture had been proposed and carried out. There have been many techniques of storing information on server storage. Such information storages furnished via cloud carrier providers have to ensure client about Confidentiality, Integrity and Availability of information. Confidentiality: Confidentiality refers to preserving records private.

Cloud Storage: Cloud storage specifies the storage on cloud with nearly inexpensive garage and backup option for small business enterprise. The real garage area may be on unmarried garage environment or replicated to more than one server storage based on importance of statistics. Typical cloud garage system structure includes a

master manage server and numerous customers. The mechanism model of cloud garage consists of four layers: storage layer which shops the facts, fundamental control layer which guarantees safety and stability of cloud storage itself, application interface layer which affords application carrier platform, and get admission to layer which offers the get entry to platform. The fundamental cloud garage environment represented as follows:

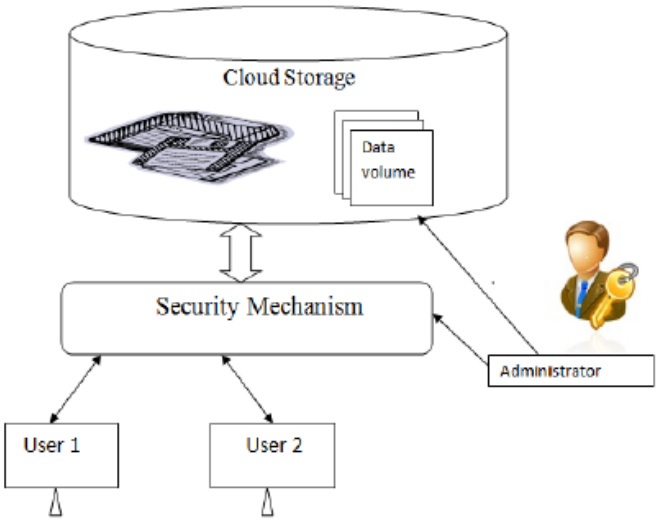

Fig 2.1: - Cloud Storage Environment

Cloud computing gives a distinguished service for statistics garage referred to as cloud garage. The go with the flow and garage of information on the cloud environment in undeniable textual content layout may be primary protection hazard. So, it's far the duty of cloud provider providers to ensure privacy and security of statistics on storage in addition to network level. The following three parameters confidentiality, integrity and availability decide whether or not security and privacy of statistics stored on cloud surroundings is maintained or not.

Cryptography application supports symmetric and asymmetric encryption set of rules to encrypt/decrypt information for importing/downloading inside cloud storage. A username and password based authentication mechanism for customers and virtual signature scheme for facts authenticity are described within cloud architecture.

Cloud computing affords on-demand aid get admission to from a shared pool of computing sources which include; hardware and software for green manage. By outsourcing the person facts to the general public cloud surroundings, this decreases the control of facts for facts owner. To maintain the manipulate of records in rest or records in movement inside networks, offers greater benefits for facts security. Protecting information inside the cloud, authentication and integrity, get entry to manipulate, encryption, integrity checking and statistics covering are a number of the records protection strategies.

Cryptography is the one of the efficient technique for statistics security in cloud computing. This includes the design and implementation of an efficient encryption and decryption algorithms. In symmetric cryptography, before outsourcing information to cloud server is encrypted into cipher text the usage of secret key and later user decrypted using equal shared secret key.

3. DES

Secrecy is at the coronary heart of cryptography. Encryption is a realistic means to attain records secrecy. Modern encryption strategies are mathematical alterations (algorithms) which deal with messages as numbers or algebraic elements in a space and rework them between a area of "meaningful messages" and a location of "unintelligible messages". A message inside the meaningful area and input to an encryption algorithm is referred to as clear text and the unintelligible output from the encryption set of rules is called ciphertext.

DES (and most of the alternative principal symmetric ciphers) is based on a cipher referred to as the Feistel block cipher. This become a block cipher advanced with the aid of the IBM cryptography researcher Horst Feistel in the early 70's. It includes a number of rounds in which every spherical contains bit-shuffling, non-linear substitutions (S-bins) and exclusive OR operations. Most symmetric encryption schemes these days are based on this structure (referred to as a feistel community).

As with maximum encryption schemes, DES expects two inputs - the plaintext to be encrypted and the secret key. The way wherein the plaintext is accepted and the important thing association used for encryption and decryption, both determines the sort of cipher it's miles. DES is consequently a symmetric, 64 bit block cipher because it uses the equal key for each encryption and decryption and best operates on sixty four bit blocks of information at a time5 (be they plaintext or ciphertext). The key size used is fifty six bits, but a 64 bit (or eight-byte) key is clearly input. The least great bit of every byte is either used for parity (peculiar for DES) or set arbitrarily and does no longer increase the security in any manner. All blocks are numbered from left to proper which makes the 8 bit of every byte the parity bit.

Once a simple-text message is received to be encrypted, it is organized into sixty four bit blocks required for input. If the wide kind of bits within the message isn't calmly divisible via sixty 4, then the very last block might be padded. Multiple diversifications and substitutions are incorporated at some stage in a good way to boom the hassle of acting a cryptanalysis on the cipher. However, it is generally ordinary that the initial and final variations provide little or no contribution to the protection of DES and in fact some software implementations leave out them.

It become followed in 1977 by the National Bureau of Standards (NBS), now National Institute of Standards and Technology (NIST), as Federal Information Processing Standard forty six (FIPS PUB 46). In 1971, IBM's crew under Horst Feistel leadership advanced set of rules LUCIFER, running on 64-bit blocks with 128-bit key. Further, IBM's crew leaded through Walter Tuchman and Carl Meyer revised LUCIFER to make it extra immune to cryptanalysis, but they reduced key size to fifty six bits. In 1973, NBS issued a request for proposals for a countrywide cipher well-known. IBM submitted outcomes of its Tuchman-Meyer task. This become via a long way the satisfactory set of rules proposed and was followed in 1977 as Data Encryption Standard. In 1994, NIST reaffirmed DES for federal use for every other 5 years. In 1999, NIST issued a new edition of its widespread (FIPS PUB forty six-three) that indicated that DES should simplest be used for legacy structures and that triple DES be used.

DES (Data Encryption Standard) set of rules reason is to offer a well-known technique for shielding touchy business and unclassified statistics. This same key used for encryption and decryption technique. DES set of rules includes the subsequent steps.

1. DES accepts an input of 64-bit long plaintext and 56-bitkey (8 bits of parity) and produce output of 64 bit block.
2. The plaintext block has to shift the bits around.
3. The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
4. The plaintext and key will processed by following
   - i. The key is split into two 28 halves.
   - ii. Each half of the key is shifted (rotated) by one or two bits, depending on the round.
   - iii. The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed keys used to encrypt this round's plaintext block.
   - iv. The rotated key halves from step 2 are used in next round.
   - v. The data block is split into two 32-bit halves.
   - vi. One half is subject to an expansion permutation to increase its size to 48 bits.
   - vii. Output of step 6 is exclusive-OR'ed with the 48- it compressed key from step 3.
   - viii. Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
   - ix. Output of step 8 is subject to a P-box to permute the bits.

4. AES

Like DES, AES is a symmetric block cipher. This manner that it makes use of the identical key for each encryption and decryption. However, AES is quite different from DES in some of ways. The algorithm Rijndael lets in for an expansion of block and key sizes and no longer just the 64 and fifty six bits of DES' block and key size. The block and key can in truth be chosen independently from 128, one hundred sixty, 192, 224, 256 bits and need no longer be the identical. However, the AES popular states that the algorithm can best accept a block size of 128 bits and a choice of 3 keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is changed to AES-128, AES-192 or AES-256 respectively. As well as those differences AES differs from DES in that it isn't always a feistel structure. Recall that in a feistel shape, half of the facts block is used to modify the opposite half of the statistics block and then the halves are swapped. In this situation the entire statistics block is processed in parallel all through each spherical using substitutions and permutations.

A quantity of AES parameters rely upon the key length. For instance, if the key length used is 128 then the number of rounds is 10 while it's far 12 and 14 for 192 and 256 bits respectively. At gift the most commonplace key size probably for use is the 128 bit key. This description of the AES set of rules consequently describes this specific implementation.

Rijndael was designed to have the following characteristics:

- Resistance against all known attacks.
- Speed and code compactness on a wide range of platforms.
- Design Simplicity.

In a primary spherical of evaluation, 15 proposed algorithms had been normal. A second spherical narrowed to 5 algorithms. NIST completed its evaluation manner and posted a final widespread (FIPS PUB 197) in November, 2001. NIST selected Rijndael because the proposed AES set of rules. The 2 researches of AES are Dr. Joan Daemon and Dr. Vincent Rijmen from Belgium.

Advanced Encryption Standard (AES) algorithm isn't always only for protection but additionally for wonderful pace. Both hardware and software implementation are quicker nevertheless. A New encryption fashionable encouraged by means of NIST to update DES is AES. Encrypts information blocks of 128 bits in 10, 12 and 14 round relying on key size. It can be applied on various platforms especially in small devices. It is carefully tested for lots securities programs.

Algorithm Steps: These steps used to encrypt 128-bit block

1. The set of round keys from the cipher key.
2. Initialize state array and add the initial round key to the starting state array.
3. Perform round = 1 to 9: Execute Usual Round.
4. Execute Final Round.
5. Corresponding cipher text chunk output of Final Round Step.

The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of it's counterpart in the encryption algorithm. The four stages are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm consist of the following:

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

Again, the tenth round simply leaves out the Inverse Mix Columns stage.

5. BLOWFISH

The statistics transformation system for Pocket Brief makes use of the Blowfish Algorithm for Encryption and Decryption, respectively. The information and working of the algorithm are given below.

Blowfish is a symmetric block cipher that may be successfully used for encryption and safe guarding of records. It takes a variable-length key, from 32 bits to 448 bits, making it best for securing records. Blowfish turned into designed in 1993 by Bruce Schneier as a quick, free alternative to present encryption algorithms. Blowfish is unpatented and license-free, and is available unfastened for all makes use of.

Blowfish Algorithm is a Feistel Network, iterating a easy encryption feature 16 times. The block length is 64 bits, and the key may be any duration up to 448 bits. Although there is a complicated initialization section required before any encryption can take place, the real encryption of facts is very green on massive microprocessors.

Blowfish is a variable-duration key block cipher. It is suitable for packages in which the key does now not exchange frequently, like a communications hyperlink or an automatic record encryptor. It is extensively quicker than maximum encryption algorithms when implemented on 32-bit microprocessors with massive records caches.

The information transformation system for Pocket Brief uses the Blowfish Algorithm for Encryption and Decryption, respectively. The info and operating of the algorithm are given underneath.

Blowfish is a symmetric block cipher that may be successfully used for encryption and safeguarding of statistics. It takes a variable-period key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish become designed in 1993 by using Bruce Schneier as a fast, loose opportunity to present encryption algorithms. Blowfish is unpatented and license-loose, and is to be had unfastened for all makes use of. Blowfish Algorithm is a Feistel Network, iterating a simple encryption feature sixteen instances. The block length is sixty four bits, and the important thing may be any length up to 448 bits. Although there is a complex initialization section required before any encryption can take vicinity, the actual encryption of facts is very green on large microprocessors.

Blowfish is a variable-duration key block cipher. It is suitable for applications where the key does now not trade often, like a communications link or an automatic record encrypt or. It is notably quicker than most encryption algorithms when implemented on 32-bit microprocessors with huge facts caches.

The Blowfish Algorithm:

- Manipulates data in large blocks.
- Has a 64-bit block size.
- Has a scalable key, from 32 bits to at least 256 bits.
- Uses simple operations that are efficient on microprocessors.

e.g., exclusive-or, addition, table lookup, modular- multiplication. It does not use variable-length shifts or bit-wise permutations, or conditional jumps.

6. PERFORMANCE EVALUATION

Several overall performance metrics are gathered: 1) Encryption time; 2) CPU method time; and 3) CPU clock cycles and battery electricity,4)Throughput,5)Different facts kinds,6)Different length of statistics block.

- **Encryption Time**

Encryption Time is considered one of a performance metric that is described as the quantity of time required for converting plaintext message to cipher textual content on the time of encryption. Encryption time is used to calculate the throughput of an encryption scheme. It shows the rate of encryption. The throughput of the encryption scheme is calculated as the whole plaintext in bytes encrypted divided by means of the encryption time.

- **Decryption Time**

Decryption Time is one in all a overall performance metric that is described as the amount of time required for changing the cipher textual content into the obvious textual content on the time of decryption.

- **Throughput**

The throughput of the encryption scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm in.

$$\text{Throughput} = \frac{\text{Total Plaintext in MegaBytes}}{\text{Encryption Time}}$$

The higher the value of throughput more is the efficiency of encrypting any text with an encryption algorithm.

- **CPU Process Time**

The CPU method time is the time that a CPU is devoted simplest to the unique method of calculations. It reflects the load of the CPU. The more CPU time is used inside the encryption technique, the better is the load of the CPU. The CPU clock cycles are a metric, reflecting the power consumption of the CPU at the same time as working on encryption operations. Each cycle of CPU will eat a small quantity of electricity.

The following responsibilities in an effort to be performed are proven as follows:

- A comparison is conducted between the results of the selected different encryption and decryption schemes in terms of the encryption time at two different encoding bases namely; hexadecimal base encoding and in base 64 encoding.
- A study is performed on the effect of changing packet size at power consumption during throughput for each selected cryptography algorithm. Key Length is an easy objective, numeric metric to adopt since key size is universally expressed as a number of bits.

In fact, every extra key bit generally doubles the number of possible keys and therefore increases the effort required for a successful brute force attack against most symmetric algorithms.

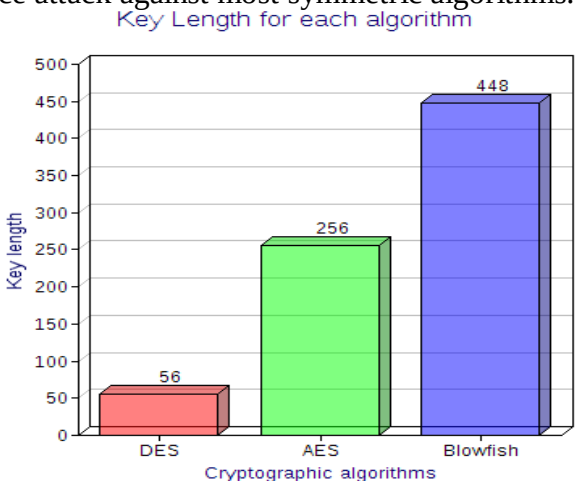

Fig 6.1: - Key Length comparison for each cryptographic algorithm

Attack Steps is defined as the wide variety of steps required to perform the first-rate recognized attack. The variety of steps facilitates decide the time that is probably required for a a hit attack, the use of a particular processor, while not having to in reality run the assault at the algorithm, which may not be feasible.

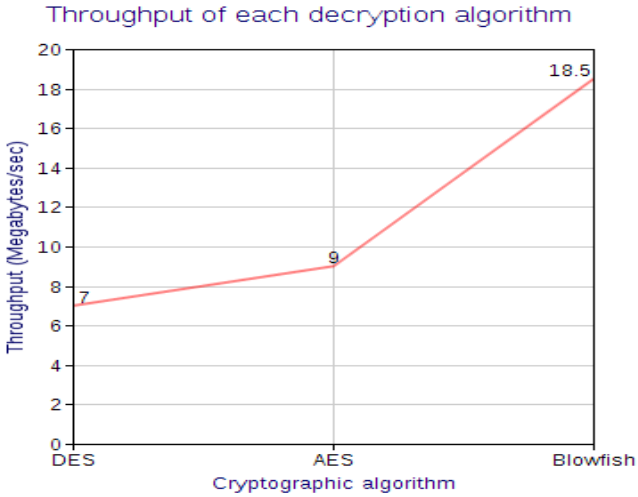

Fig 6.2: - Throughput for each cryptographic algorithm

The performance matrices are encryption and decryption time. The encryption time is defined as the time that an encryption algorithm takes to generate a cipher text from simple textual content and decryption time is described as the time that an encryption algorithm takes to generate undeniable text from cipher textual content.

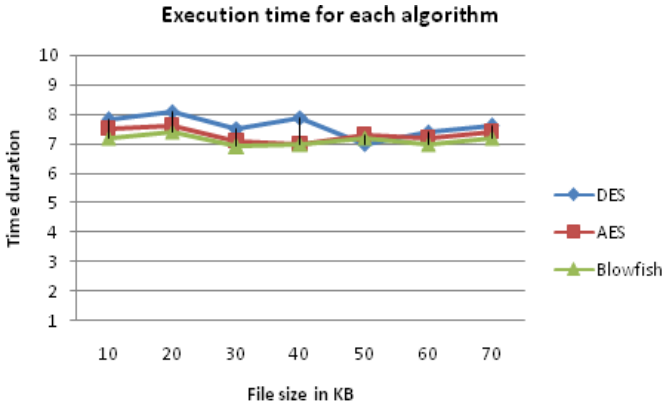

Fig 6.3: - Execution time for each cryptographic algorithm

Algorithm power became selected because the name of a scale developed for expressing the overall dimension of a cryptographic set of rules's strength, well worth or cost, even though the size has to be defined and expressed in subjective, adjectival phrases. This is the most effective subjective, adjectival characteristic scale for set of rules specification that becomes developed in the course of this pilot. The Algorithm Strength (AS) metric is intended for use by using skilled cryptographers to specify, or explicit an evaluation of, set of rules energy values.

Determination of algorithm strength need to take into consideration the first-class regarded methods of assault and the length of time required to carry out the ones attacks the use of contemporary generation.

7. CONCLUSION

The goal of the paper is to offer a overall performance analysis among symmetric key cryptography algorithms: DES, AES and Blowfish. The analysis has been carried out by jogging several encryption settings to process distinct sizes of information blocks to evaluate the set of rules's pace for encryption and decryption. Each algorithm is designed and completed in these modes. The variant is furnished in information length given

by the consumer. The statistics is retrieved from various text documents to calculate the time fed on via every set of rules to system the retrieved statistics.

The provided simulation outcomes showed that Blowfish has a better overall performance than other commonplace encryption algorithms used. Since Blowfish has not any recognised security susceptible factors thus far, this makes it an exceptional candidate to be taken into consideration as a popular encryption set of rules. AES confirmed poor overall performance outcomes in comparison to different algorithms since it requires greater processing strength.

REFERENCES

[1] M. Abdalla, M. Bellare, and P. Rogaway, "The oracle Diffie-Hellman assumptions and an analysis of DHIES," in *Topics in Cryptology – RSA Conference Cryptographers' Track (RSA-CT 2001)*, vol. 2020 of *Lecture Notes in Computer Science*, pp. 143–158, Springer-Verlag, 2001.

[2] G. Anastasi, A. Falchi, A. Passarella, M. Conti, and E. Gregori, "Performance measurements of motes sensor networks," in *Proceedings of the 7th International Symposium on Modeling Analysis and Simulation of Wireless and Mobile Systems (MSWiM 2004)*, pp. 174–181, ACM Press, 2004.

[3] R. Anderson and M. Kuhn, "Tamper resistance–a cautionary note," in *Proceedings of the 2nd USENIX Workshop on Electronic Commerce*, pp. 1–11, USENIX Association, 1996.

[4] "Anonymity and Privacy in Electronic Services (APES), IWT/STWW Project." *h*https://www.cosic.esat.kuleuven.ac.be/apes/*i*.

[5] D. Balfanz, G. Durfee, N. Shankar, D. K. Smetters, J. Staddon, and H. C. Wong, "Secret handshakes from pairing-based key agreements," in *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pp. 180–196, IEEE, 2003.

[6] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," in *Advances in Cryptology - CRYPTO 2002*, vol. 2442 of *Lecture Notes in Computer Science*, pp. 354–368, Springer-Verlag, 2002.

[7] D. J. Barrett, R. E. Silverman, and R. G. Byrnes, *SSH, The Secure Shell: The Definitive Guide, Second Edition*. O'Reilly, 2005.

[8] L. Batina, J. Lano, N. Mentens, B. Preneel, I. Verbauwhede, and S. B. ¨ Ors, "Energy, performance, area versus security trade-offs for stream ciphers," in *ECRYPT Workshops – The State of the Art of Stream Ciphers (SASC 2004)*, pp. 302–310, 2004.

[9] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proceedings of the 1th ACM Conference on Computer and Communications Security (CCS 1993)*, pp. 62–73, ACM Press, 1993.

[10] M. Bellare and P. Rogaway, "Optimal asymmetric encryption," in *Advances in Cryptology - EUROCRYPT 1994*, vol. 950 of *Lecture Notes in Computer Science*, pp. 92–111, Springer-Verlag, 1995.

[11] M. Bellare and P. Rogaway, "The exact security of digital signatures: How to sign with RSA and Rabin," in *Advances in Cryptology – EUROCRYPT 1996*, vol. 1070 of *Lecture Notes in Computer Science*, pp. 399–414, Springer-Verlag, 1996.

[12] M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," in *Advances in Cryptology - ASIACRYPT 2000*, vol. 1976 of *Lecture Notes in Computer Science*, pp. 531–545, Springer-Verlag, 2000.

