SIPARUNTON
International Journal of
Interdisciplinary Research

ISSN 2337-0556 (Print)
ISSN 2337-0572 (Online)
Vol 1, Issue 2, October 2012

Increasing the security of e-commerce systems using some models of combined cryptography

Florim IDRIZI
Department of IT, Faculty of Math-Natural Sciences, Tetovo State University

Ilia NINKA
Department of IT, Faculty of Natural Sciences, University of Tirana

Abstract

Secure communications are an important precondition of e-commerce transactions and are required for confidential electronic communications. Every e-commerce system relies on encryption to secure data transmission by controlling data access and protect information on the internet and ultimately boost consumer confidence. By implementing encryption, integrity is maintained while digital authentication is enforced, thus allowing both customers and merchants to verify the identity of the other party, a concept fundamental to secure online credit card transactions. In this paper we will explain the basic concepts of encryption and the needs and opportunities of using several cryptographic systems. Next, we will present some of the most recent algorithms which are supporting and enabling these confidential electronic communications. At the same time we will compare and evaluate individual algorithms by taking into consideration the security aspect and their complexity.

Keywords: e-commerce, digital authentication, encryption, cryptographic systems, cryptography

1. Introduction

The notion of securing messages through cryptography has a long history. Julius Caesar is credited with creating one of the earliest cryptographic systems to send secret military messages to his generals. Throughout history, however, there has been one central problem limiting widespread use of cryptography. That problem is key management. In cryptographic systems, the term key refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information. Consequently, the term key management refers to the secure administration of keys to provide them to users where and when they are required**.**

Any business that wants to have a competitive edge in today's global marketplace should adopt a comprehensive security policy in consultation with partners, suppliers, and distributors that will provide safe environment for the coming proliferation of E-commerce [1].

Internet has made the idea of an idealized marketplace seem presumptive and credible. However, there are still turmoil and concerns regarding the exchange of money safely and conveniently over the Internet. This research is undertaken primarily to explore the benefits of using some of the most well known cryptographic algorithms as a method of E-commerce security, and secondly to determine the benefits and gains of encryption methods and techniques to secure internet E-commerce. We start the paper by giving a theoretical background at section two. Further, we continue to illustrate some algorithms such as: Digital Encryption Standard (DES), Triple DES, AES, RSA and DSA. At section four we compare and evaluate some of these algorithms and at the last section we provide some conclusions.

1. Basic concepts of cryptography- literature review

Cryptography helps us to store sensitive and classified information or transmit it across insecure and vulnerable networks so that it can reach safely the destination.

Cipher systems are classified into 2 classes which are: 1- Secrete key cipher system, 2- Public-key cipher system. In the following we shall describe each class briefly.

Secret key cryptography is the oldest type of method in which to write things in secret. There are two main type of secrete key cryptography, transposition and substitution. Transposition cipher, encrypt the original message by changing characters order in which they occurred. Whereas in substitution cipher, the original message was encrypted by replacing there characters with other characters. In both types, both the sender and receiver share the same secret keys. The most widely used secret key scheme today is called Data Encryption Standard (DES). DES cipher work with 56-bit secret key and 16 rounds to transform a block of plaintext into ciphertext . [2]

1.1 Encryption and decryption

Data that can be read and understood without any special measures is called plaintext or cleartext. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext. The encryption is used to ensure that information is hidden from anyone for

whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption.

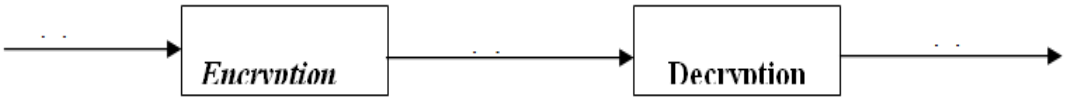

Figure 1. Encryption and Decryption

Plaintext is denoted by M, for message, or P, for plaintext. It can be a stream of bits, a text file, abitmap, a stream of digitized voice, a digital video image whatever. As far as a computer is concerned, M is simply binary data. The plaintext can be intended for either transmission or storage. In any case, M is the message to be encrypted. Ciphertext is denoted by C. It is also binary data: sometimes the same size as M, sometimes larger. (By combining encryption with compression, C may be smaller than M. However, encryption does not accomplish this.) The encryption function E, operates on M to produce C. Or, in mathematical notation:

$$E(M) = C$$

In the reverse process, the decryption function D operates on C to produce M:

$$D(C) = M$$

Since the whole point of encrypting and then decrypting a message is to recover the plaintext, the following identity must hold true: [3]

$$D(E(M)) = M$$

1.2 Digital Signatures

Using Digital signature a message can be signed by a device using its private key to ensure authenticity of the message. Any device that has got the access to the public key of the signed device can verify the signature. Thus the device receiving the message can ensure that the message is indeed signed by the intended device and is not modified during the transit. If any the data or signature is modified, the signature verification fails.[4]

Digital Signature is a method to encrypt a message (such as documents, contracts, notifications) which will be transferred, adopting data-exchanging protocol and data-encrypting algorithm. An abstract is produced in this procession. the abstract is like signature or seal which can be used by receiver to verify the identity of the sender [5]. The functions of digital signature: 1- Assuring data integrity. Once the message changes a little, the abstract will change a lot for hash function's peculiarity, so that avoids the message being distorted. 2 – Anti - denibility. Using public key cryptography algorithm, the sender can't deny that he has sent the message for he has the private key. 3 - Avoiding receivers forging message that is claimed to be from the sender.

For example, a computer system can deal with time and date by adding time stamp to a file automatically. Digital signature scheme is secure, because these schemes are based on encrypting technology usually and the security relies on the concrete algorithm. Common digital signature algorithm should assure that the signature is anti-deniable, anti-repeated and the message is impossible to be changed. The signature should resist all kinds of existing attack [6]

1.3 Digital Certificates

In an environment where it is safe to freely exchange keys via public servers, man-in-the-middle attacks are a potential threat. In this type of attack, someone posts a phony key with the name and user ID of the user's intended recipient. Data encrypted to— and intercepted by—the true owner of this bogus key is now in the wrong hands. In a public key environment, it is vital that you are assured that the public key to which you are encrypting data is in fact the public key of the intended recipient and not a forgery. You could simply encrypt only to those keys which have been physically handed to you. But suppose you need to exchange information with people you have never met; how can you tell that you have the correct key? Digital certificates, or certs, simplify the task of establishing whether a public key truly belongs to the purported owner. A certificate is a form of credential. Examples might be your driver's license, your social security card, or your birth certificate. Each of these has some information on it identifying you and some authorization stating that someone else has confirmed your identity. Some certificates, such as your passport, are important enough confirmation of your identity that you would not want to lose them, lest someone use them to impersonate you. A digital certificate is data that functions much like a physical certificate. A digital certificate is information included with a person's public key that helps others verify that a key is genuine or valid. Digital certificates are used to thwart attempts to substitute one person's key for another. A digital certificate consists of three things: 1. A public key, 2. Certificate information. ("Identity" information about the user, such as name, user ID, and so on), 3.One or more digital signatures.

The purpose of the digital signature on a certificate is to state that the certificate information has been attested to by some other person or entity. The digital signature does not attest to the authenticity of the certificate as a whole; it vouches only that the signed identity information goes along with, or is bound to, the public key.[10]

Although digital certificates are widely adopted by major businesses, certificate practices may not be completely secure. Although digital certificates guarantees the uniqueness of the website that users are interacting with, the relationship between the certificate owner, the website

operator, and the website content owner may be vague and therefore not guaranteed. Research has shown that authentication and authorization should also be separated as much as possible even though digital certificates accommodate authorization information within their fields [7]

3. Some cryptographic algorithms in e-commerce

E-Commerce security requirements can be explored by examining the overall process, starting with the consumer and ending with the commerce server. Taking into account each logical link in the "commerce chain", the assets that must be protected to ensure secure e-commerce involve client computers, the messages travelling on the communication channel, and the web and commerce servers – including any hardware attached to the servers. While telecommunications are certainly one of the major assets to be protected, the telecommunications links are not the only concern in computer and e-commerce security. For instance, if the telecommunications links were made secure but no security measures were implemented for either client computers or commerce and web-servers, then no communications security would exist at all.[8]

3.1 Digital Encryption Standard (DES)

Before applying DES the text is split up into the 64 bit blocks. DES applied on each 64 bit block.
Encryption method is described below.
Step 1: Apply an initial permutation on a block.Result is *B=IP(P)* where *P* is the 64 bit block *IP* Initial Permutation function and B the result.
Step 2: Split *B* into 32 bit blocks
Li = leftmost 32 bits,
Ri = rightmost 32 bits.
Step 3: Pick a 56 bit key. Permute it
Step 4: Left circular shift it by 1 bit giving K_1.
Step 5: Perform a complex sequence of operations and obtain $X_1 = F(R_1,K_1)$ (The complex set of operations include table look up and dropping bits).
Step 6: *Find* $R_2 = L_1 + X_1$
Step 7: *Set* $L_2 = R_1$
Repeat steps 2 to 7 16 times to get $B_{16} = L_{16},R_{16}$
Step 8: Apply inverse of initial permutation on B_{16}
The result is the encrypted block shown below:

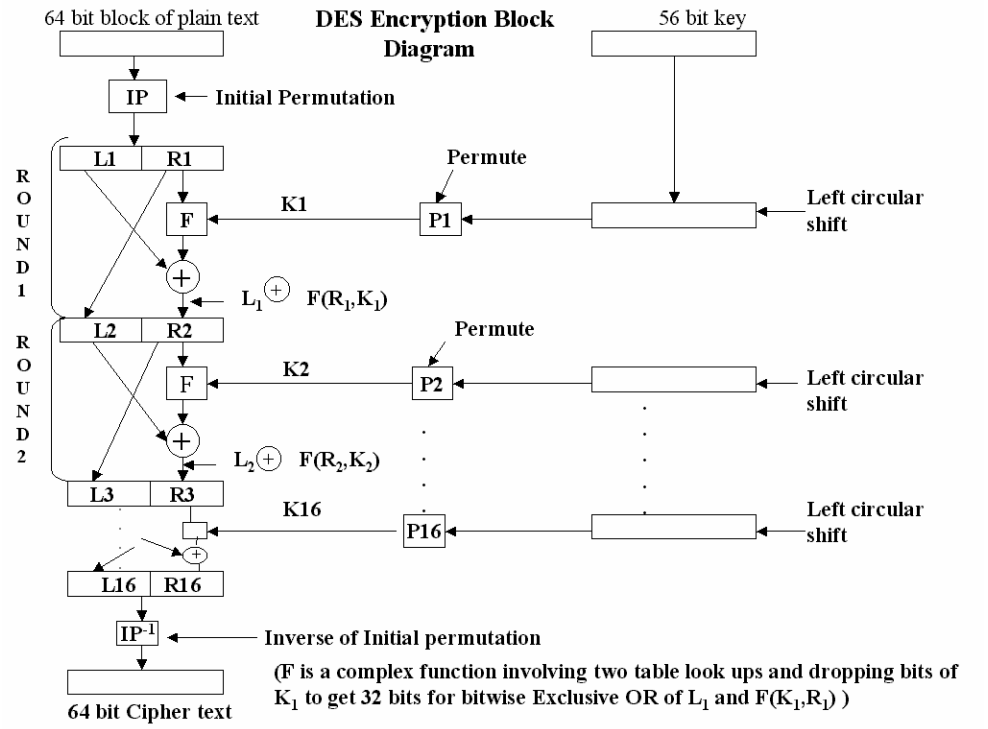

Figure 2. Encrypted block using DES

In summary the DES encryption applies the following transformation 16 times. The ith round transformation are

$$L_{i+1} = R_i$$

$$R_{i+1} = L_i \oplus F(R_i,K_i)$$

Each round has a different key Ki For Decryption the process of encryption is reversed. The encrypted block is permuted using IP^{-1}.On this transformations are applied starting with K_{16} and going to K_1 last. The keys and F are same as those used in encryption process.[9]

Cryptanalysis is technique for breaking a code, given the samples of encrypted messages. If plain text is also known it is somewhat easier. DES code can be broken if key is found. The easiest method of breaking a code is by brute force of trying out all possible keys to decrypt message. With increase in speed of computers it has now been shown that DES key can be found in less than 12 hrs with a fast computer (1 million decryption per microsecond). Thus DES is practically useless now (original DES was invented in mid 70s). New more secure

symmetric encryption algorithm is needed. An extension of DES called triple DES is tested to be more secure. [9]

3.1.1 Example Of DES Use

M = PLAINTEXT 01010011 11110000 10101010 11001100
K = KEY 11101001 01101111 01110011 01001111

ENCRYPTION - $E = M \oplus K = \overline{M}K + M\overline{K}$ 10111010 10011111 11011001 10000011

DECRYPTION - $M = E \oplus K = \overline{E}K + E\overline{K}$ 01010011 11110000 10101010 11001100

3.2 Triple DES

Triple DES uses three different keys and three executions of DES algorithm.
The algorithm is: *Cipher text = E_{k3} [D_{k2} [E_{k1} [Plain Text]]]*
where *E_k[X] = DES Encryption of X using key K*
and *D_k[X] = DES Decryption of X using key K*.
We saw that in DES Decryption of encrypted plain text with a different key is almost same as another encryption. This is true as encryption and decryption use the same algorithm. To decrypt cipher text we reverse the operations.
Plain text = D_{k1}[E_{k2} [D_{k3}[Cipher Text]]]
Using DES thrice is equivalent to having a DES key length of 168 bits. Brute force method to break triple DES with 10^6 decrypts per micro second will take 5.9 X 10^{30} years! Even at 10^{12} fold increase in computer speed will make triple DES secure against brute force attacks to break code. The only reason D is used as middle step in triple DES is to allow decryption of data encrypted using single DES hardware. In this case K_3=K_2=K_1 (Single key used).
Triple DES will be quite popular for a foreseeable future as it is very secure, can be realised by simple hardware. Triple DES has two disadvantages: 1) It is slow to implement in software, 2) It uses 64 bit blocks. [9]

3.3 Digital Signature Algorithm (DSA)

In August 1991, The National Institute of Standards and Technology (NIST) proposed the Digital Signature Algorithm (DSA) for use in their Digital Signature Standard (DSS). According to the Federal Register [11]:
A Federal Information Processing Standard (FIPS) for Digital Signature Standard (DSS)is being proposed. This proposed standard specifies a public-key digital signature algorithm (DSA) appropriate for Federal digital signature applications. The proposed DSS uses a public key to verify to a recipient the integrity of data and identity of the sender of the data. The DSS can also be used by a third party to ascertain the authenticity of a signature and the data associated with it.
This proposed standard adopts a public-key signature scheme that uses a pair of transformations to generate and verify a digital value called a signature.
And:
This proposed FIPS is the result of evaluating a number of alternative digital signature techniques. In making the selection NIST has followed the mandate contained in section of the Computer Security Act of 1987 that NIST develop standards to "...assure the cost-effective security and privacy of Federal information and, among technologies offering comparable protection, on selecting the option with the most desirable operating and use characteristics." Among the factors that were considered during this process were the level of security provided, the ease of implementation in both hardware and software, the ease of export from the U.S., the applicability of patents, impact on national security and law enforcement and the level of efficiency in both the signing and verification functions. A number of techniques were deemed to provide appropriate protection for Federal systems. The technique selected has the following desirable characteristics: NIST expects it to be available on a royalty-free basis. Broader use of this technique resulting from public availability should be an economic benefit to the government and the public.
The technique selected provides for efficient implementation of the signature operations in smart card applications. In these applications the signing operations are performed in the computationally modest environment of the smart card while the verification process is implemented in a more computationally rich environment such as a personal computer, a hardware cryptographic module, or a mainframe computer. Before it gets too confusing, let me review the nomenclature: DSA is the algorithm; the DSS is the standard. The standard employs the algorithm. The algorithm is part of the standard. [3]

3.3.1 Description of DSA

The algorithm uses the following parameters:
p = a prime number L bits long, when L ranges from 512 to 1024 and is a multiple of 64.
(In the original standard, the size of p was fixed at 512 bits [12]. This was the source
of much criticism and was changed by NIST [13].)
q = a 160-bit prime factor of *p – 1.*
g = $h^{(p-1)/q}$ mod p, where h is any number less than *p – 1* such that $h^{(p-1)/q}$ mod p is
greater than 1.
x = a number less than *q.*
y = g^x mod p.
The algorithm also makes use of a one-way hash function: H(m). The standard specifies the Secure Hash Algorithm.
The first three parameters, *p, q,* and *g,* are public and can be common across a network of users. The private key is *x* the public key is *y*.
To sign a message, m:
(1) Alice generates a random number, k, less than q.
(2) Alice generates
r = (g^kmod p) mod q
s = (k^{-1} (H(m) + xr)) mod q
The parameters *r* and *s* are her signature; she sends these to Bob.
(3) Bob verifies the signature by computing
w = s^{-1} mod q
*u_1 = (H(m) * w) mod q*

$u_2 = (rw) \bmod q$
$v = ((g^{u1} * y^{u2}) \bmod p) \bmod q$
If $v = r$, then the signature is verified [3]

3.4 Advanced Encryption Standard (AES)

In 1990s NIST (National Institute of Statndards and Technology) began its effort to develop the AES, which is a symmetric key encryption algorithm, and made a world wide public call for the algorithm to succeed DES.
The AES algorithm is a subset of the Rijndael algorithm. The AES algorithm uses a 128 bit block and three different key sizes 128, 196 and 256 bits, where Rijndael allows multiple block sizes 128, 196, and 256 bits and for each it also allows multiple key sizes, again 128, 196, and 256 bits. The AES algorithm is a symmetric key algorithm which means the same key is used to both encrypt and decrypt a message. Also, the cipher text produced by the AES algorithm is the same size as the plain text message.

3.5 RSA Algorithm

The RSA algorithm generates public and private key pair by the following method. Two sufficiently large prime numbers are selected and multiplied together with its product stored, or $n = p * q$, where n is also known as the modulus. Another number e less than n is chosen, with the characteristics of being relatively prime to $(p-1)(q-1)$; in other words, e and $(p-1)(q-1)$ only have 1 as the common factor. An additional number d is selected such that $(ed-1)$ is divisible by $(p-1)(q-1)$ where e*d = 1 mod (p-1)(q-1). In this case, e and d correspond to the public and private exponents respectively while the public key is the pair (n, e) and the private key is (d). [7]
RSA Code Details."R" Wants To Find His Public And Private Keys
1. Pick large primes p and q. Let $n = p * q$
2 Find $ø = (p-l)*(q-l)$
3 Find e relatively prime to $Ø$, *i.e.* $gcd(ø,e)=1; 1<e<ø$. {e,n} is R's Public Key
4 Find a number d which satisfies relation
$(d * e) \bmod (ø) = 1$
{d,n} is R's Private key
5. Let *plain text* = *t*. Encrypt **t** using R's public key.
Encryption = $t^e \pmod n = c$ (cipher text)
6.Decryption $c^d \pmod n = t$

3.5.1 Example Of RSA Use

This example is a toy example to illustrate the method. In practice the primes p and q will be very large – each at least 300 digits long to ensure security.
1.We pick as prime numbers $p=3, q=11$
$n = p * q = 33$
We should note that the message which is to be encrypted should be smaller than 33.If we do letter by letter encryption of English alphabets (A to Z as 1 to 26) this is OK
2. $Ø = (p-1) \times (q-1) = 2 \times 10 = 20$
3.We pick a number relatively prime to 20.
We pick 7. The Public key of $R = \{7,33\}$
4.To pick private key of R find d from relation $(d \times e) \bmod (ø) = 1$
$(d \times 7) \bmod (20) = 1$
This gives d =3. Therefore, the private key of $R = \{3,33\}$[9]

3.5.2 Applying RSA Algorithm

1.Let the message is **ERDIT**. If we use code E=5, R=18, D=4,I=9, T=20, than the message is 5,18,4,9,20.
2.We will **encrypt** one letter at a time. Thus cipher of plain text 3 is
$5^e \bmod (n) = 5^7 \bmod (33)$
$E - (5^7) \bmod (33) = 78125 \bmod (33) = 14$
$R - (18)^7 \bmod (33) = 612220032 \bmod (33) = 6$
$D - (4)^7 \bmod (33) = 16384 \bmod (33) = 16$
$I - (9)^7 \bmod (33) = 4782969 \bmod (33) = 15$
$T - (20)^7 \bmod (33) = 1280000000 \bmod (33) = 26$
3.Thus cipher text = 14,6,16,15,26
4. **Decryption**: $c^d \bmod (n)$ d=3,n=33
$E - 14^3 \bmod (33) = 2744 \bmod (33) = 5$
$R - 6^3 \bmod (33) = 216 \bmod (33) = 18$
$D - 16^3 \bmod (33) = 4096 \bmod (33) = 4$
$I - 15^3 \bmod (33) = 3375 \bmod (33) = 9$
$T - 26^3 \bmod (33) = 17576 \bmod (33) = 20$
We see that we get the original text 5,18,4,9,20

3.4.3 Combining RSA and DES

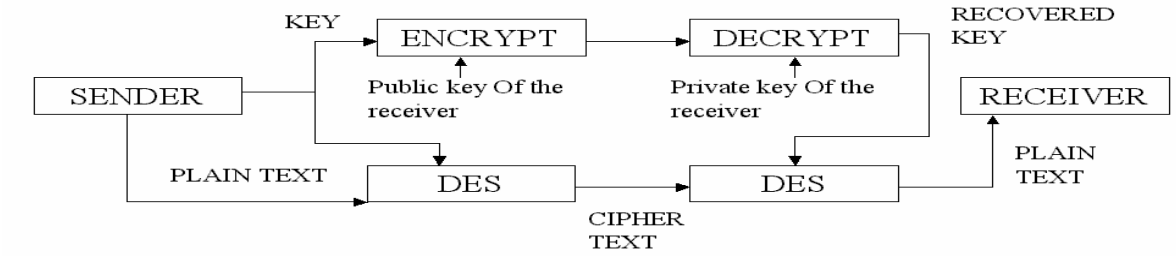

Figure 3. Combining RSA and DES algorithms

Here key is sent along with the plain text. Encrypted using RSA. Key is small-fast to encrypt/decrypt and each transaction using DES can have a different key- higher security and also fast. The key directory not needed. [9]

4. Comparison and evaluation of algorithms in terms of transactional security

In this section we try to compare these algorithms in terms of transactional security. RSA Public key has two keys – a private secret key and a public open key. RSA is implemented as a program (software). It is computationally complex to encode plain text and decode cipher text using RSA DES Same key for encryption and decryption. It is a single key system - Also called symmetric key system. DES computationally simple-implemented in hardware - thus very fast Each communication between two businesses can use a different key – provided key is securely exchanged. If key can be sent separately encrypted using RSA, then a recipient can use this to decrypt DES encrypted message. [9]

DSA is faster for signature generation but slower for validation, slower when encrypting but faster when decrypting and security can be considered equivalent compared to an RSA key of equal key length. That's the punch line, now some justification. The security of the RSA algorithm is based on the fact that factorization of large integers is known to be "difficult", whereas DSA security is based on the discrete logarithm problem. Today the fastest known algorithm for factoring large integers is the General Number Field Sieve, also the fastest algorithm to solve the discrete logarithm problem in finite fields modulo a large prime p as specified for DSA. Now, if the security can be deemed as equal, we would of course favour the algorithm that is faster. But again, there is no clear winner.

One of the most well-known and most widely used symmetric encryption algorithms is Data Encryption Standard (DES). DES typically operates in block mode, where it encrypts data in 64-bit blocks. Like other symmetric algorithms, DES uses the same algorithm and key for both encryption and decryption. DES has stood the test of time. Cryptography researches have scrutinized it for nearly 35 years and so far have found no significant flaws. Adding to its appeal, because DES is based on relatively simple mathematical functions, it may be easily implemented and accelerated in hardware.

quote: The key length of AES is much stronger than that of DES. and AES runs much faster than 3DES on comparable hardware. With these features, AES was chosen to replace DES and 3DES. AES is also better suited for high-throughput, low-latency environments. This is especially true when pure software encryption is used.

In terms of longevity, AES is a relatively young algorithm. As mentioned previously, a more mature algorithm is always more trusted. That being the case, 3DES represents a more conservative yet more trusted choice in terms of strength, because it has been analyzed for nearly 35 years.

quote: As mentioned, DES, with its original 56-bit key, is too short to withstand even medium-budget attackers. One means of increasing the security of DES without changing the well-analyzed algorithm itself is to use the same algorith but with different keys multiple times in a row. In essence, that is what 3DES does. [14] AES is a symmetric block cipher algorithm, the successor of the des. It's used to encode files, documents, etc. It works fast and is very sure. For encoding and decoding you use the same key. If you wish to use AES for communication (enocde a message), the receiver has to have the key, so there is a key exchange problem. This problem is solved using asymmetric algorithms like RSA. Here the sender encodes a message using a private key. The receiver decodes the message with the public key. Everyone can use this public key. So, the receiver can decode the message. Asymmetric algorithms are quite slow, so key exchange works with asymmetric algorithms, encoding of data with symmetric algorithms. Both are quite easy to implement. [15]

5. Conclusion

In this paper we discussed the basic concepts of encryption and the needs and opportunities of using several cryptographic systems. We analyzed and introduced some of the most well known algorithms which support and enhance the transactional security. At the last section of the paper, we compared and evaluated each algorithm by taking into account the security and implementation aspects and their complexity.

E-commerce has become heavily reliant on PKI technology to boost consumer's confidence and safeguard their most fundamental assets—business data and customer's personal information. Public key encryption emerged as superior over private key encryption for online transactions as it eliminates the need for secret key exchange. Combined with the strengths of digital signatures/certificates and the SSL protocol, a consumer's online experience becomes more secure through key establishment and server authentication, reducing the risks associated with online data theft.

References

[1] Dave Chaffey, "E-Business and E-Commerce", 2nd , Prentice Hall, 2005
[2] Nada M. A. Al-Slamy E-Commerce security, IJCSNS International Journal of Computer Science and Network 340 Security, VOL.8 No.5, May 2008
[3] B. Schneier, Applide Cryptography, protocols, algotithms,and source code on C.
[4] T. Elxsi, Public Key Cryptography, Applications Algorithms and Mathematical Explanations
[5] Malkin T, Micciancio D, Miner S. Effcient Generic Forward-secure Signatures with an Unbounded Number of Time Periods[C]. Proc. Of Advances in Cryptology-EUROCRYPT. 2002
[6] Hongjie Zhu, Daxing Li, Research on Digital Signature in Electronic Commerce. Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol I IMECS 2008, 19-21 March, 2008, Hong Kong
[7] Diana W. E-commerce Security, Encryption Methods for secure e-commerce websites.

[8] A Sengupta, C Mazumdar M S Barik, e-Commerce security – A life cycle approach. Vol. 30, Parts 2 & 3, April/June 2005, pp. 119–140. © Printed in India
[9] Electronic Commerce http://nptel.iitm.ac.in/courses/Webcourse-contents/IISc-BANG/System%20Analysis%20and%20Design/pdf/Lecture_Notes/LNm13.pdf
0] An Introduction to Cryptograph, ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf
[11] "Proposed Federal Information Processing Standard for Digital Signature Standard (DSS)," Federal Register, v. 56, n. 169, 30 Aug 1991, pp. 42980-42982.
[12] National Institute of Standards and Technology, NIST FIPS PUB XX, "Digital Signature Standard," U.S. Department of Commerce, DRAFT, 19 Aug 1991.
[13] National Institute of Standards and Technology, NIST FIPS PUB 186, "Digital Signature Standard," U.S. Department of Commerce, May 1994.
[14] http://www.dslreports.com/forum/r26896261-DES-vs-AES
[15] http://security.ittoolbox.com/documents/aes-vs-rsa-13016