Improvements in field of Encryption and Decryption by focusing on Time attack

Aarushi Singhal, Divya Batra

Abstract

Security is one of the most important thing. When data is uploaded online and is being transmitted from one place to another then it becomes vulnerable to attacks and if correct measures are not taken then it causes leakage of sensitive information. Ranging from compression to symmetric methods and now asymmetric method for encrypting data has significantly substantiated ways to give security at different levels.

The symmetric technique for encryption focused on transference of data using key management by encrypting and decrypting data by same key which did not provide security to data at major level, as use of same key for encryption and decryption can easily be leaked if data is leaked. This called for new methods to be introduced which could provide such encryption technique that could help in saving data from different attacks and can't easily be leaked.

RSA , an asymmetric cryptographic technique is one of such methods which has reduced the leakage of data by introducing 2 different keys for data encryption and decryption. One key is public that is accessible to all and the other one is private key which is only accessible to the person whom it belongs to and is not shared with others.RSA has made transmission of data easy online without any leakage as it ensures that the person who has valid key can only decrypt message. The non transference of keys has enhanced its security. As it is majorly used technique adding more level of security to it is must. So concentrating on removing problems such as time attack etc and enhancing scope of security even if the private key is lost.

Key Points: Cryptography, public key cryptography, RSA, attacks, Digital signature

1.Introduction

Public key cryptography is a cryptographic technique in which 2 keys are involved for transmission of message from one place to another. One is called public key and other is called private key. Unlike symmetric key cryptography, in public key cryptography there is no need to transmit key with the transmission of data and thus we can save key from being leaked. Public key is known to all, but private key works as a secret key which is saved with the person and is not shared. If public key is used to encrypt the message then private key of the particular person is required to decrypt the message and vice versa. No other private key can decrypt the message and thus it:

a. authenticated the sender who has sent the message.

b. key leakage risk factor is reduced which makes it less susceptible to loss of information or being attacked in the way of transmission of message.

c. sense of security makes it world-wide used method for encryption.

One of the public key cryptography is RSA. RSA is an encryption algorithm which stands for Rivest Shamir Adlemen, based on the last names of the scientists who made this algorithm in the year 1977. This algorithm designed to remove the disadvantage of symmetric key in which key is same for encryption and decryption and can be leaked on the way of transmission with data. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

2.RSA Algorithm

The RSA cryptosystem is the most widely-used public key cryptography algorithm in the world. It can be used to encrypt a message without the need to exchange a secret key separately.
The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers.
Party A can send an encrypted message to party B without any prior exchange of secret keys. A just uses B's public key to encrypt the message and B decrypts it using its private key, which only he knows. RSA can also be used to sign a message, so A can sign a message using his private key and B can verify it using A's public key.
A user wishing to exchange encrypted messages using a public-key cryptosystem would place their public encryption procedure, E, in a public file. The user's corresponding decryption procedure, D, is kept confidential. Rivest, Shamir, and Adleman provide four properties that the encryption and decryption procedures have:

- Deciphering the enciphered form of a message M yields M. That is, D(E(M)) = M
- E and D are easy to compute.
- Publicly revealing E does not reveal an easy way to compute D. As such, only the user can decrypt messages which were encrypted with E. Likewise, only the user can compute D efficiently.
- Deciphering a message M and then enciphering it results in M. That is, E(D(M)) = M

As Rivest, Shamir, and Adleman point out, if a procedure satisfying property (3) is used, it is extremely impractical for another user to try to decipher the message by trying all possible messages until they find one such that E(M) = C.
[1]

Algorithm:

1. Choose two different large random prime numbers p and q

2. Calculate n = pq

   - n is the modulus for the public key and private keys

3. Calculate the totient : $\phi(n) = (p-1)(q-1)$.

4. Choose an integer e such that $1<e<\phi(n)$, and e is co-prime to $\phi(n)$ I.e. e and $\phi(n)$ share no factors other than 1; $\gcd(e, \phi(n))=1$.

   - e is released as the public key exponent.

5. Compound d to satisfy the congruence relation $de =1 \pmod{\phi(n)}$ i.e.: $\mathbf{de=1+k\phi(n)) = 1.}$

   - d is kept as the private key exponent.

6. To encrypt the message

$$\mathbf{C=M^e \bmod(\phi)}$$

7. To decrypt the cipher text

$$\mathbf{M = C^d \bmod(\phi))}$$

$$\mathbf{M=M^{ed} \bmod(\phi)}$$

Refer to step 5 for finding value of 'd'

3.Objective

Although RSA is one of the best algorithm used for transference of the message from one place to another but still it has some problems:

a. Key size is very big which increases overhead and also increases time for encryption and decryption.

b It is Susceptible to time attack.

c. If key is leaked then RSA algorithm will hold no good.

d. It is prone to side channel attacks.

e. Small values of p and q results in guessing of key much easier, so their respective has to be 1024 bit length at least.

4.M-RSA

One of the main thing associated with any encryption algorithm is its safety and security, RSA has although conquered the Brute Force but still other attacks such as time attack has endangered its security, so there is a need to improve RSA in matter of security for its betterment.

RSA is susceptible to attacks like time attack which is very dangerous as it without getting into code attacker tries to guess the value of key or value of 'd' by the reference of time of computations taken by program to run.

So modified version of RSA or modified -RSA concentrates on making code more secure by securing 'd' and making cryptographic message more difficult to find out.

For enhancement of security

once the cipher text is generated using normal RSA then it is again being shuffled and rotated by the number of rounds stated by receiver in his OTP message which is 4 bit encryption key which can vary in length (for demonstration it is taken to be 4 bit length), here the main feature is that even if the key of receiver is lost then also hacker will only have access to private key of receiver but he won't be able to decipher the number of rounds the cryptographic message is shuffled and rotated. These number of rounds will be known to sender and receiver in the form of one time password generated initially so even if hacker having access to private key of receiver he won't get the real message.

Use of shuffling technique and rotation to randomize the value of cipher text and also making it difficult for hacker to predict the real text (plain text) as the receiver first specify number of rounds to the sender which the sender will apply to shuffle and rotate the cipher text once it is generated after implementation of RSA.

Randomized selection of the value of p and q within a certain limit so that key length could be difficult to estimate at the beginning only. Key length is equal to size of addition of p and q which are two prime numbers. They are generally kept of equal size to minimize the complexity in calculation

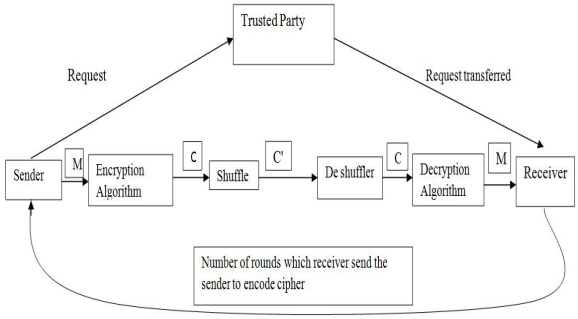
As RSA on 512 bits key length is being broken by the brute force attack so we have implemented this technique on 1024 bits key length which finally comprises the result key of length 2048 .

5.Algorithm of M RSA

1. First the sender sends a request to third party which acts as mediator that he wants to set a communication link with the particular receiver.
2. The third party then transfers the same request to the receiver regarding connection communication. Receiver then sends a message encrypted with public key of sender

describing the number of rounds he desires for encrypting cipher text in the form of "One time Password" or "OTP".
3. Sender then decrypts the OTP message using his private key.
4. The whole process of RSA applies which includes formation of key, encryption of message.
5. Then once the cipher text is generated it then is circularly rotated to the left by 1 and then arranged in a form of matrix without leaving any space vacant, if any number is left in key then it is removed ,once the matrix is formed it is shuffled and after that the key is taken out with left over part concatenated into it, this makes one round and this process is repeated number of times the receiver has specified in OTP (round key).
6. After the last round the new cipher text is created which is transmitted to the receiver and there receiver applies the whole process in reverse order to track plain text.

Fig 5.1Diagrammatic representation of MRSA algorithm:



where:

M = message or plain text

C= cipher Text formed after applying RSA

C'= after rounding and shuffling of C number of times specified in OTP

Fig5.2Pictorial Representation showing flow of control

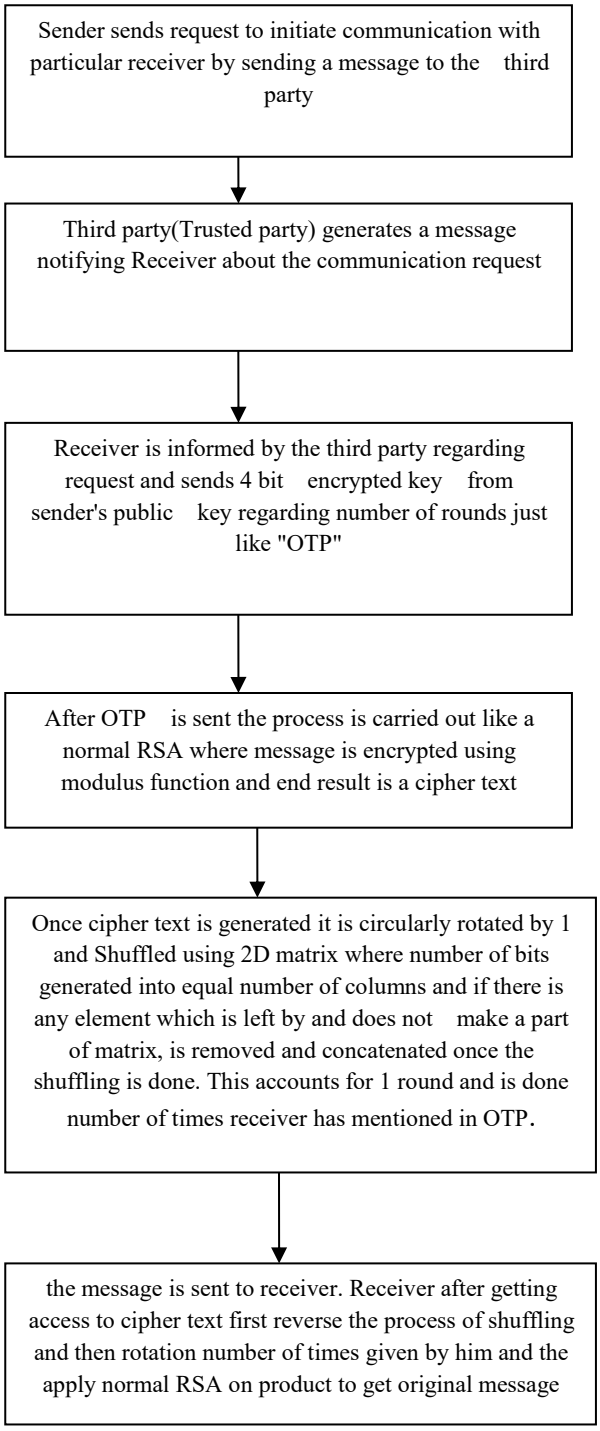
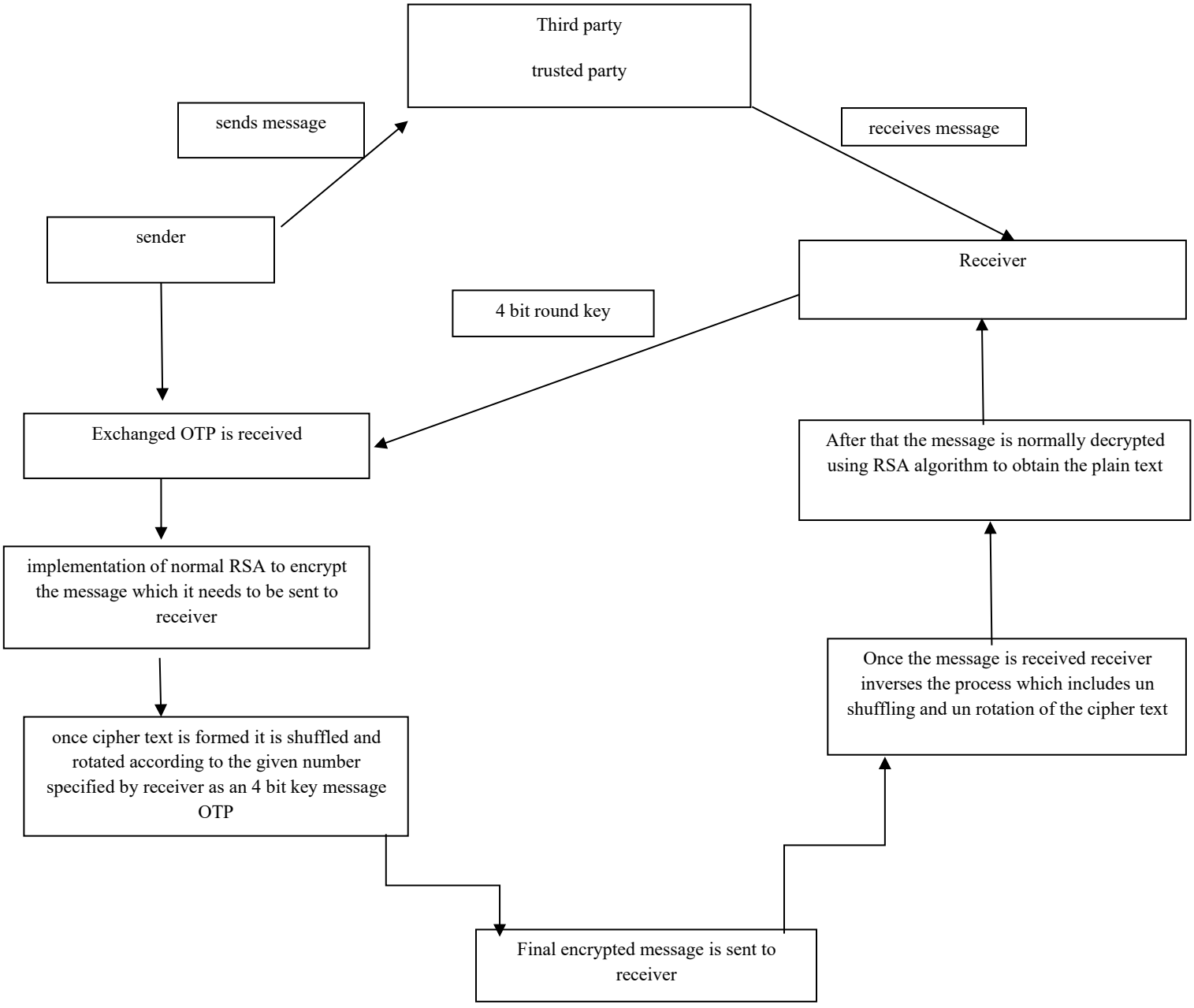


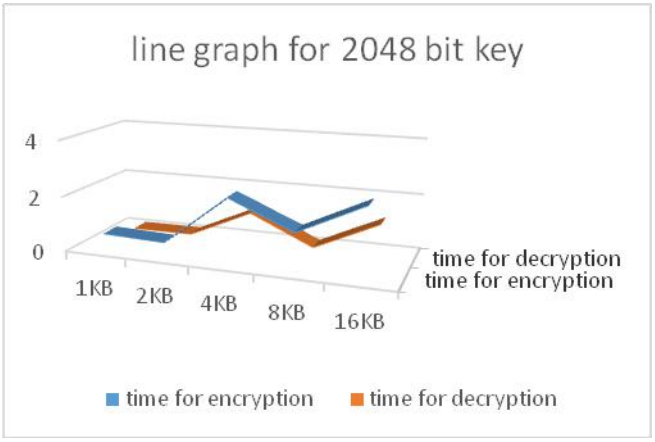
Fig 5.3 Block diagram:



6.Observations and graph

Serial NO.	Key Length (bits)	Encrypting Time (seconds)	Decrypting Time (seconds)	Size of Message (kilobyte)
1	2048	0.57	0.12	1 KB
2.	2048	0.492	0.132	2 KB
3.	2048	2.311	1.17	4 KB
4.	2048	1.46	0.12	8 KB
5.	2048	2.46	1.2	16 KB

Table 6.1 OBSERVATION TABLE OF RSA 2048 BITS KEY LENGTH



Graph (5.a) Time for encryption & decryption in RSA (Time versus Data size)
(2048-bit key length)

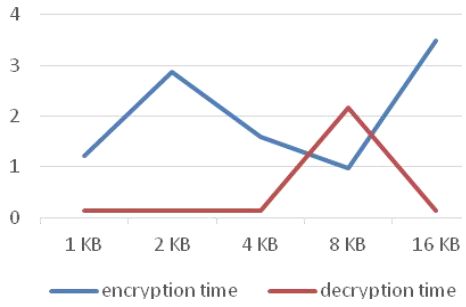
Description:

This graph shows that as the file size increases so the time of encryption increases and as the time of encryption increases, time of decryption also increases thus giving a somewhat similar linear equation as that of time of encryption.

This graph shows both the time encryption as well as decryption is directly proportional to each other.

S. No.	Key Length	Encrypting Time (in sec)	Decrypting Time (in sec)	Size of Message
1.	2048	1.211	0.122	1 KB
2.	2048	2.88	0.128	2 KB
3.	2048	1.58	0.122	4 KB
4.	2048	0.977	0.17	8 KB
5.	2048	3.50	0.122	16 KB

Table 6.2 OBSERVATION TABLE OF M-RSA FOR 2048 KEY LENGTH



Graph (5.b) Time for encryption & decryption in MRSA (Time versus Data size)
(2048-bit key length)

Description:

This graph shows that as the file size increases so the time of encryption but the time of decryption remains almost constant because of which time attack based on finding key on the basis of time of computation has rather become difficult.

This graph shows that encrypting and decrypting time is not linear and decrypting time almost remain constant which enhance security and save it from time attack.

Table6.3

COMPARISON WITH RSA

S.No	Modified RSA comparison with RSA	Improvements
1.	**Security**	The major focus is laid on enhancement of security in modified RSA. The methods of shuffling and rotation encrypt cipher text to more number of rounds to enhance security
2.	**Key size**	Key is changed from big decimal to hexadecimal to reduce its size. Hexadecimal provides same level of functions as big decimal but it reduces key size to some extent which not only make computations effective but also reduces overhead. It shortens the time of encryption and decryption of message.
3.	**Third party Authentication**	Involvement of third party to authenticate sender and receiver who will be engaged in communication by sending and verifying request.

7.Summary

1. The message can be entered in ASCII format.

2. Use of shuffling technique and rotation to randomize the value of 'd' and also making it difficult for hacker to predict the real text (plain text) as the receiver first specify number of rounds to the sender which the sender will apply to shuffle and rotate the cipher text once it is generated. The value of number of rounds cipher text is being computed is only know to sender and receiver, and thus it leads to enhancement of security. even if the key of receiver is misplaced or hacked then in that are also the hacker will not be aware of the additional shuffling and rotation done on cipher text for how many number of rotations. The message promoted by the receiver will be of same format as that of OTP generation. Once the transaction and message transmission is over the OTP is automatically released.

3. use of varying range of size of p and q instead of taking it closer to each other helps in enhancing security as it makes make brute force difficult t apply from the start.

4. conversion of key from big decimal to hexadecimal to reduce key size to same extent and also overhead is reduced.

8.Conclusion:

1. Brute Force : The size of key taken is 2048 which provides extensive amount of security from brute force in immediate future.

2. As number of computations are increased by shuffling and rotating the cipher text it has provided new level of security, time attack focuses on observing time of computation, sound analysis, cipher text etc. MRSA focuses on increasing number of computations on the basis of hidden analysis of One Time Password which refers to number if rounds.

One round comprises of shuffling and circular rotation of the cipher text(C) generated after the RSA has been applied once to generate cipher text(C').

The cipher text is first divided into equal number of columns and then is shuffled to give another cipher text(C') and number of rounds will be stated by receiver.

3. Third party authentication: Both receiver as well as sender has to be registered under trusted party for transference of request. Third party or trusted party keeps details of both sender and receiver, so this brings and keeps transparency in the process of transference of message.

It is sender who sends request to third party to set communication link with the respected receiver and third party notifies receiver regarding the request made by sender.

4. Generation Of session Key: Generation of round key or session key by receiver sent to sender to carry out process of MRSA, is unique and effective because it generates only one session for whole process to be carried out in safe and secure environment.

5. Time of decryption almost remain constant which makes it more secure from time attack irrespective of RSA where encryption time and decryption were linearly increasing with increase n file size

9.References

[1] Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". *Communications of the ACM* **21**

[2] Paul C Kocher "Timing Attacks on Implementation of Diffie-Hellman, RSA, DSS and Other Systems"

[3] Prime Number Hide-And-Seek: How the RSA Cipher Works.

[4] Cryptography world / RSA Copyright 2004. Papers, ISO 17799, ITIL, Sarbanes-Oxley, Etal

[5] P.Saveetha and S.Arumugam ,"Study on Improvements in RSA Algorithm and its implementation" Volume 3, ISSUE 6, 7,8,2012

[6] William Stallings ,"Cryptography and Network Security" ISBN 81-7758-011- Pearson Education ,Third Edition.

[7] Joshi Maitri and Fenil Khatiwala ,"Survey of Different Modifies RSA technologies and Analysis", International Journal Of Engineering Technology Management and Applied Science Volume 3, ISSUE 2, ISSN 2349-4476 February , 2015

[8] Israt John, Mohammad Asif, Liton Jude Rozario, "Improved RSA Cryptosystem based on the study of number theory and public key cryptosystems" American Journal Of Engineering Research (AJER), e -ISSN 2320-0847, p- ISSN 2320-0936 Volume 4, ISSUE 1, 2015

[9] Hinek M.J.: On the security of some variants of RSA. PhD.thesis, University of Waterloo, Waterloo(2007)

[10] Hoffstein J., Pipher J., Silverman J.H.:An Introduction to Mathematical Cryptography Springer, Berlin(2008)

[11] Dhananjay Pugila, Harsh Chitrala, Salpesh Lunawat , P.M.Durai Raj Vincent "An Efficeient Encrpytion Algorithm Based On Public Key cryptography" International Journal of Engineering and Technology (IJET) , Vol 5 No 3 Jun-Jul 2013.

[12] Bidzos, Jim, "Threats to Privacy and Public Keys for Protection", *COMPCON Spring '91 Digest of Papers*, IEEE Computer Society Press, p. 189-94