Diss/07/02/197

The RSA Public Key Cryptography, its implementation issues and analysis of the possible attacks against the same

A dissertation submitted in partial fulfillment of the requirements for the completion of degree of the Master of Technology in Computer Science (2005-2007)

by

Arijit Bhattacharyya (mtc0501)

Under the supervision of

Subhamoy Maitra

ASU, Indian Statistical Institute .

2007

Indian Statistical Institute
203, B.T. Road, Kolkata – 108

Synopsis of dissertation titled "**The RSA Public Key Cryptography , its implementation issues and analysis of the possible attacks against the same "**

by
Arijit Bhattacharyya (mtc0501)

Under supervision of Subhamoy Maitra , ASU , Indian Statistical Institute .

❖ Introduction

Cryptography , the subject of data security has been evolved a lot from the very early time of human communication . As the civilization progressed , more and more sophisticated ways to encrypt data have been designed . Beside that , the effort of breaking the secure data by the unauthorized people has also succeeded a lot . Naturally some new cryptosystems were required when the existing ones showed weakness . Public key cryptography has been much more popular than the symmetric key protocols since its invention . In this context , the RSA system have got the most success due to its seemingly unbreakable implementation , designed by Ron Rivest , Adi Shamir and Len Adleman . Though it is used still today in highly sensitive and crucial security purposes , its principle of unbreakability is based on the fact that factoring large integers is still infeasible even by the fastest computers ever designed so far . Moreover , careless design and parameter choosing may harm the essence of security of the same . In this paper , we do a survey on the implementation issues of the RSA protocol , some efficiency measures and the failure cases in particular situations , step by step .

❖ Background to implement the cryptosystem

We begin by describing the Euclidean algorithm , Extended Euclidean algorithm and computing Jacobi symbol along with their programming implementation . Modular exponentiation method is extremely useful to make the encryption and

decryption procedures much faster and we implement it in our design . As we know , to generate the RSA primes , we need to choose some large random numbers first and then check for their primality . We analyze some randomized techniques for checking primality and note some experimental results . First Solovay-Strassen and then the most popular one – Miller-Rabin algorithm . We also notice the result of these two algorithms side by side , by giving the same input to them .

❖ Factoring integers , algorithms and some classic attacks on RSA

Next we move forward and begin the possible approaches to attack the cryptosystem . Factoring a large number with some non-negligible probability might help us in this effort , so we study two popular but old methods – the p-1 and the Rho algorithm , both due to Pollard . We note their complexity and run with some random integers , Whenever we are unable to factor the input integer , we check it by Miller-Rabin whether it's a prime indeed or not , according to the latter algorithm .Then we discuss one of the most efficient methods of recent time , the Quadratic Sieve algorithm due to Carl Pomerance .
These method is one of the most efficient factoring procedures , and most of the cases it responds in acceptable time with positive result , though the parameters which are used in the algorithm , may speed up efficiency if chosen properly , on the other hand may reduce the success probability .We mention one more problem , computing half(C) , which is , like the problem of factoring large integers efficiently , can be reduced to finding the RSA inverse by a definite procedure .

Then we analyze an extremely useful breaking strategy of the RSA protocol using the continued fraction expansion of rational numbers , when small decryption exponent is used in RSA , due to M. Wiener . We implement it in our programme and show some experimental results . Here we modify our Euclidean algorithm a bit , to meet our necessity . We keep track of the remainders in all the steps to compute the convergents later . Most of the powerful attacks against RSA while low public exponent e is used , are based on an important theorem by Coppersmith . We prove the theorem and in the context we discuss the LLL algorithm by Lenstra , Lenstra and Lovesz .

Hastad used the Chinese Remainder theorem to show that if the same message is broadcasted to different persons , then one could recover the original plaintext if the number of ciphertexts captured is greater than the value of the encryption key . We write down the code for implementing Chinese Remainder Theorem here . Then we study the Franklin-Reiter attack in case of related messages . We do mention some other possibilities at the end .

Using very large RSA private exponent also poses a threat which we discuss in the next section . We already know that using small decryption exponent in RSA implementation is vulnerable of Wiener's attack , which is very practical in real applications. But in fact this and some other attacks are feasible even if the decryption exponent is very large, i.e., in the other extreme. Instead of using large value for decryption exponent, one may tempt to use small negative value corresponding to the high key-value to reduce the modular exponentiation time. In fact , complexity of computing C^{-d} mod n and then taking the inverse, so just an addition of one extra inversion modulo N . We discuss those issues here along with the attack due to Bleichenbacher and May. We conclude with a recent attack on RSA for d_p and d_q being bounded by certain limit .

❖ Conclusion

The RSA Cryptosystem , since its invention , has been widely used in number of applications where security and authentication of digital data is concerned . Although , different people have put much effort to break this cryptosystem , in the last 30 years since its invention , no such devastating strategy exists till date . Most of them describes the dangers in improper implementation of RSA . Even the existence of some probabilistic algorithm , they don't show any feasible and promising solution to break the protocol and RSA is still one of the best choices . But the cryptanalysists , are on their way to crack the system and till now , using primes of 512 bits length are still safe , along with taking care of the values of the exponents .