Mathematics Today Vol.32 (June & December 2016) 61-66
ISSN 0976-3228

Studying Exponentiation Cipher Modulo a Composite Number

D. R. Sanyasi[1] and Nittal Patel[2]

[1]Gujarat Arts And Science College, Ahmedabad, India
E-mail: devendrachemical@gmail.com.
[2]Department of Science and Humanities,
Shankersinh Vaghela Bapu Institute of Technology,
Gandhinagar, India
E-mail: nittalbpatel000@gmail.com.

Abstract

In the past few years there were several eye-catching attacks on the security of RSA, but none were able to pose a continuous threat to it. Pohlig and Hellman invented an idea of exponentiation in ciphers and considered a prime modulus. In this paper, exponentiation cipher is explored modulo composite numbers of type p^2q and p^2q^2 and the study suggests that they too can serve as good ciphers.

Keywords: Exponentiation cipher, Cryptography, Pohlig-Hellman cipher, Modular arithmetic in application

AMS Classification 2010: 11T71

1 Introduction

Cryptography is a science of communicating in presence of an adversary. One of the most widely applied and used public key cryptography technique is RSA cryptosystem. The mathematical aspect responsible for well being of RSA cryptosystem is the unavailability of a sufficiently fast running (i.e. polynomial time reduction) algorithm to factor a large number [2]. The usefulness of RSA cryptosystem in some sense is due to impragnable nature of RSA due to above property. Numerous attempts were made in order to develop more and more, fast as well as accurate tools and procedures to factor a large composite number since the advent of RSA. But still a polynomial time reduction algorithm is awaited. This is why RSA is widely in use for very high quality secret message sending. In and around same time when RSA was discovered, Pohlig and Hellman invented an idea of exponentiation in ciphers [8]. In the exponentiation

cipher, at the sender's end, the desired plaintext after converting to related number sequence is then subdivided into various strings of suitable size depending on the size of an odd prime modulus p. It is further raised to a random positive integer (less than the size of modulus) modulo p. This gives rise to ciphertext. A similar procedure at the receiver's end is followed to obtain the plaintext message in quick time, provided the receiver has knowledge of inverse of the random positive integer used during encryption. The modulus chosen in exponentiation cipher is a prime number whereas the modulus chosen in RSA is a sufficiently large composite number, which is a product of two primes of almost same size [1]. Exponentiation cipher modulo a prime number is only of theoretical importance, because obtaining private key from the public key is easy using extended Euclidean algorithm [4]. In this paper, exponentiation cipher is explored modulo composite numbers of type p^2q and p^2q^2 and the findings are interesting in the sense that they also serve as good ciphers.

2 Preliminaries

The definitions 2.1 to 2.6 given below are referred from [5, 9] and the theorems 2.7 to 2.9 are from [4].

Definition 2.1 PLAINTEXT [5, 9] *is the original form of information to be transmitted by one party to another party.*

Definition 2.2 CIPHERTEXT [5, 9] *is the camouflaged form of information which is actually received by the receiver party.*

Definition 2.3 ENCRYPTION [5, 9] *is an algorithmic procedure by which a given plaintext message is transformed into ciphertext.*

Definition 2.4 DECRYPTION [5, 9] *is an algorithmic procedure by which a ciphertext is converted back to its respective plaintext message form.*

Definition 2.5 PRIVATE KEY [5, 9] *is that secret associated with encryption algorithm which does not allow the ciphertext to be transformed back to plaintext without its knowledge. It is also sometimes referred to as a secret key.*

Definition 2.6 ADVERSARY *or* INTRUDER [5, 9] *is an unintended third party other than sender and receiver party which may obtain some or all parts of data transmitted over an insecure channel. We assume an adversary to be equipped with the most powerful computational resources.*

Theorem 2.7 Fermat's Little Theorem [4]*: Let p be a prime number and a be an integer with $p \nmid a$. Then $a^{p-1} \equiv 1 (\text{mod } p)$.*

Theorem 2.8 Euler's Theorem [4]*: Let a and n be integers with $n > 1$ and $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 (\text{mod } n)$.*

Theorem 2.9 [4] *A positive integer $n > 1$ can be factored as $n = xy$ for some positive integers x, y if and only if there exist positive integers a, b with $n = a^2 - b^2$.*

Fermat-Kraitchik factorization technique in [4], a straight forward application of theorem 2.9 is a good attempt towards factorizing large numbers but is not fast enough. Fermat-Kraitchik method was also tried along with probabilistic approach of selecting the seeds, but was not very promising [7].

3 Notations

In the entire article from here onwards, P will denote the universe of all plaintext messages and C will denote the universe of all ciphertext messages. Also M will denote the universe of all numerical equivalents of elements of P. Let $\mathcal{A}$ be the set of all alphabets. Without loss of generality let us consider the set $\mathcal{A}$ to be collection of alphabets A-Z (all capitals) and $\mathbb{J} := \{00, 01, 02, \ldots, 25\}$. To obtain the numerical equivalent of an element of P, first of all we define a natural injective map $f : \mathcal{A} \to \mathbb{J}$ such that $f(\text{A}) = 00, f(\text{B}) = 01, f(\text{C}) = 02, \ldots, f(\text{Z}) = 25$. This natural map can be changed as per the need and the complexity desired. In all, there are 26! possibilities for functions of type $f : \mathcal{A} \to \mathbb{J}$ in above case of sets $\mathcal{A}$ and $\mathbb{J}$ that are injective. Everywhere in the article, Alice and Bob may point to a firm or an entity and not necessarily an individual.

4 Modified Exponentiation Cipher

4.1 Exponentiation cipher with modulus p^2q

Suppose Alice wishes to transmit plaintext message $\alpha \in P$ to Bob securely over an insecure channel. So Alice will first of all convert α to its numerical equivalent say $\beta \in M$ using the function $f : \mathcal{A} \to \mathbb{J}$ defined above. On the other hand Bob is to consider two sufficiently large odd prime numbers p and q and make p^2q public along with a positive integer κ_1 satisfying $\gcd(\kappa_1, (p^2 - p)(q - 1)) = 1$. If for some $t \in \mathbb{N}$,

$$10^{2t} + 10^{2(t-1)} + \cdots + 10^2 + 1 < \frac{p^2q}{25} \leq 10^{2(t+1)} + 10^{2t} + \cdots + 10^2 + 1$$

then at Alice's end the numerical equivalent $\beta = x_1x_2\dots x_m$, for some m and $x_i \in \{0,1,\dots,9\}$ for all $i = 1,2,\dots,m$ is converted into r smaller strings say $\gamma_1,\gamma_2,\dots,\gamma_r$ of $2t$ decimal digits each. Here

$$r = \begin{cases} \frac{m}{2t} & \text{if} \quad 2t|m \\ \lceil \frac{m}{2t} \rceil & \text{if} \quad 2t \nmid m \end{cases}$$

where the deficient digits (if $2t \nmid m$) in the last string will be taken as any digits of Alice's choice. Then γ_j for each $j = 1,2,\dots,r$ is converted into a ciphertext string using the relationship $\xi_j \equiv {\gamma_j}^{\kappa_1} (\text{mod } p^2q)$ with $0 \leq \xi_j < p^2q$. In this way, Alice prepares ciphertext message $\lambda = \xi_1\xi_2\dots\xi_r$ which is sent to Bob over an insecure channel. On receiving the ciphertext, Bob who has the knowledge of p and q both, obtains $\kappa_1^{-1} (\text{mod } (p^2-p)(q-1))$ by the use of Extended Euclid's algorithm given in [4]. Let $\kappa_1^{-1} = \psi_1$ i.e.

$$\kappa_1^{-1} \equiv \psi_1 (\text{mod } (p^2-p)(q-1)) \Longrightarrow \kappa_1\psi_1 = 1 + \mu_1(p^2-p)(q-1)$$

for some μ_1. By applying Theorem 2.8 and using ψ_1, Bob will obtain γ_j from ξ_j for each $j = 1,2,\dots,r$.

$${\xi_j}^{\psi_1} \equiv ({\gamma_j}^{\kappa_1})^{\psi_1} \equiv {\gamma_j}^{\kappa_1\psi_1} \equiv {\gamma_j}^{1+\mu_1(p^2-p)(q-1)} \equiv \gamma_j({\gamma_j}^{(p^2-p)(q-1)})^{\mu_1} \equiv \gamma_j (\text{mod } p^2q)$$

These γ_j's will then be transformed to $\alpha \in P$ by re-utilizing the transformation f.
An adversary on the other hand with the knowledge of public key (p^2q, κ_1) only, cannot decipher the encrypted message λ without obtaining κ_1^{-1}. And to obtain κ_1^{-1}, an adversary will require to know the prime factors of modulus p^2q. But this factorization for a large composite number is a hard problem and different values of κ_1 determine different ciphers. So this cipher is safe to use.

4.2 Exponentiation cipher with modulus p^2q^2

Suppose Alice wishes to transmit plaintext message $\alpha \in P$ to Bob securely over an insecure channel. So Alice will first of all convert α to its numerical equivalent say $\beta \in M$ using the function $f : \mathcal{A} \to \mathbb{J}$ defined above. On the other hand Bob is to consider two sufficiently large odd prime numbers p and q and make p^2q^2 public along with a positive integer κ_2 satisfying $\gcd(\kappa_2, (p^2-p)(q^2-q)) = 1$. If for some $t \in \mathbb{N}$,

$$10^{2t} + 10^{2(t-1)} + \dots + 10^2 + 1 < \frac{p^2q^2}{25} \leq 10^{2(t+1)} + 10^{2t} + \dots + 10^2 + 1$$

then at Alice's end the numerical equivalent $\beta = x_1x_2\dots x_m$, for some m and $x_i \in \{0,1,\dots,9\}$ for all $i = 1,2,\dots,m$ is converted into r smaller strings say $\gamma_1,\gamma_2,\dots,\gamma_r$ of $2t$ decimal digits

each. Here

$$r = \begin{cases} \frac{m}{2t} & \text{if} \quad 2t|m \\ \lceil \frac{m}{2t} \rceil & \text{if} \quad 2t \nmid m \end{cases}$$

where the deficient digits (if $2t \nmid m$) in the last string will be taken as any digits of Alice's choice. Then γ_j for each $j = 1, 2, \ldots, r$ is converted into a ciphertext string using the relationship $\xi_j \equiv {\gamma_j}^{\kappa_2} (\text{mod } p^2q^2)$ with $0 \leq \xi_j < p^2q^2$. In this way, Alice prepares ciphertext message $\lambda = \xi_1\xi_2 \ldots \xi_r$ which is sent to Bob over an insecure channel. On receiving the ciphertext, Bob who has the knowledge of p and q both, obtains $\kappa_2^{-1} (\text{mod } (p^2 - p)(q^2 - q))$ by the use of Extended Euclid's algorithm given in [4]. Let $\kappa_2^{-1} = \psi_2$ i.e.

$$\kappa_2^{-1} \equiv \psi_2 (\text{mod } (p^2 - p)(q^2 - q)) \Longrightarrow \kappa_2\psi_2 = 1 + \mu_2(p^2 - p)(q^2 - q)$$

for some μ_2. By applying Theorem 2.8 and using ψ_2, Bob will obtain γ_j from ξ_j for each $j = 1, 2, \ldots, r$.

$${\xi_j}^{\psi_2} \equiv ({\gamma_j}^{\kappa_2})^{\psi_2} \equiv {\gamma_j}^{\kappa_2\psi_2} \equiv {\gamma_j}^{1+\mu_2(p^2-p)(q^2-q)} \equiv \gamma_j({\gamma_j}^{(p^2-p)(q^2-q)})^{\mu_2} \equiv \gamma_j (\text{mod } p^2q^2)$$

These γ_j's will then be transformed to $\alpha \in P$ by re-utilizing the transformation f.
An adversary on the other hand with the knowledge of public key (p^2q^2, κ_2) only, cannot decipher the encrypted message λ without obtaining κ_2^{-1}. And to obtain κ_2^{-1}, an adversary will require to know the prime factors of modulus p^2q^2. But this factorization for a large composite number is a hard problem and different values of κ_2 determine different ciphers. So this cipher is safe to use.

5 Conclusion

1970 onwards many mathematicians and computer scientists joined the race in search for a good technique to factor large composite numbers [1], [7], [6]. To name a few M. A. Morrison, J. Brillhart, John Pollard, H. W. Lenstra [6], [3]. It is well known that in the RSA algorithm, the modulus is a product of two large primes. Dan Boneh in [1] writes that in the past few years there were several fascinating attacks on the security of RSA, but none were devastating. In fact, the attacks were actually suggesting the improper use of RSA. Mathematically speaking, this precisely means that factoring a large composite is still a hard problem and large numbers of type p^2q and p^2q^2 will both require high amount of computational resource and time. So if in the Pohlig Hellman's exponentiation cipher, the prime modulus is replaced by a composite number of type described in 4.1 and 4.2, then both these algorithms can serve as good ciphers for use where data security is of high concern.

6 Acknowledgements

The authors would like to acknowledge with deep sense of gratitude the DST-FIST (Department of Science and Technology - Fund for Improvement of Science & Technology infrastructure) support (Grant # MSI - 097) to the Department of Mathematics, Gujarat University, Ahmedabad, where the first author is registered as a Ph.D. student and the second author was an M.Phil. student when this work was carried out.

References

[1] Boneh D.: *Twenty Years of Attacks on the RSA Cryptosystem*, 1998.

[2] Boneh D. and Venkatesan R.: *Breaking RSA may not be equivalent to factoring*, In EUROCRYPT '98, Springer-Verlag, 1998.

[3] Buhler J. P., Lenstra H. W. Jr. and Pomerance Carl: *Factoring Integers with the Number Field Sieve*, available for reference at the following web address "https://openaccess.leidenuniv.nl/bitstream/handle/1887/2149/346?sequence=1", 1993.

[4] Burton David M.: *Elementary Number Theory*, Tata McGraw Hill, 2007.

[5] Das Abhijit and Madhavan C. E. Veni: *Public-Key Cryptography: Theory and Practice*, Pearson Education, 2009.

[6] Morrison Michael A., Brillhart John: *A Method of Factoring and the Factorization of* F_7, Mathematics of Computation, Vol 29, No. 129, Jan 1975.

[7] Pomerance Carl: *A Tale of Two Sieves*, Notices of the AMS, Vol 43, No. 12, Dec 1996.

[8] Rosen Kenneth H.: *Elementary Number Theory and Its Applications*, Pearson Addison Wesley, Page 305-307, 2004.

[9] Shyamala C. K., Harini N. and Padmanabhan T. R.: *Cryptography and Security*, Wiley India, 2011.