2012 International Conference on Industrial and Intelligent Information (ICIII 2012)
IPCSIT vol.31 (2012) © (2012) IACSIT Press, Singapore

An Encryption Algorithm Based on the Prime Roots of Unity

Aaron Koch [1], Nidhal Bouaynaya [1+], Roman Shterenberg [2] and Radu F. Babiceanu [1]

[1] Department of Systems Engineering, University of Arkansas at Little Rock, USA
[2] Department of Mathematics, University of Alabama at Birmingham, USA

Abstract. We propose a new encryption algorithm, which uses the cyclic group of the prime roots of unity as its fundamental architecture. We show that the tangent values of the angles of the prime roots of unity are irrational, and therefore, can be used to encrypt characters in a seemingly random manner. Furthermore, we show that the group can be rotated while still preserving the irrationality of the tangent values. We associate the characters, to be encrypted, with digits in each of the irrational numbers. Breaking the proposed encryption algorithm amounts to a complexity of the order factorial of the prime number, $p!$. In particular, attacks can be made computationally prohibitive by choosing a large prime number. The proposed algorithm is illustrated for text encryption.

Keywords: encryption, prime roots of unity, cyclic groups

1. Introduction

One of the first great advances in public key cryptography is the RSA algorithm, named after its inventors Ron Rivest, Adi Shamir and Leonard Adleman [1]. RSA is based on the prime factorization of an integer, which is a difficult problem for large integers given that no efficient integer factorization algorithm is known. The public key of the RSA consists of two integer values m and k. The private key consists of prime values p and q whose product equals m. The RSA encryption algorithm associates the characters in the message with numbers on the set 1, 2, ..., $m - 1$, and then groups the numbers together and raises them to the power k modulo m. In order to decrypt the message, it is necessary to know the prime factorization of the integer m as the product of the two primes p and q in the private key. With these two primes it is possible to find the Euler Phi function value of m and raise the transmitted group to this power to recover the k^{th} root and therefore decrypt the message. Since knowledge of the prime factors of m is all that is required to decrypt RSA encrypted data, a hacker with the ability to find the factors of m will have all of the information necessary to decrypt an RSA encrypted transmission. That is why it is necessary to select p and q so that m is sufficiently large to make its factorization computationally difficult. Since its development, different versions of the RSA algorithm have been proposed [2 - 4]. Currently, RSA is widely used in electronic commerce protocols.

In this paper we propose a novel encryption system which also relies on the property of prime numbers, but unlike the RSA algorithm, uses the prime roots of unity as its fundamental architecture. The architecture of the proposed encryption consists of distributing the character set over the prime divisions of a circle located at the prime roots of unity, as depicted in Fig. 1. We associate each character with the tangent of a prime root angle on the circle. We show that the advantage of using the tangent of the angle of the p^{th} roots of unity is that this tangent value is irrational when p is prime (except for the identity which has no character associated with it). Since irrational numbers have an infinite decimal expansion and pseudorandom sequences can be obtained from expansion of irrational numbers [5], we can associate the characters with digits of the irrational number in a seemingly random manner.

+ Corresponding author. Tel.: + 501-683-7666; fax: +501-569-8698.
E-mail address: nxbouaynaya@ualr.edu.

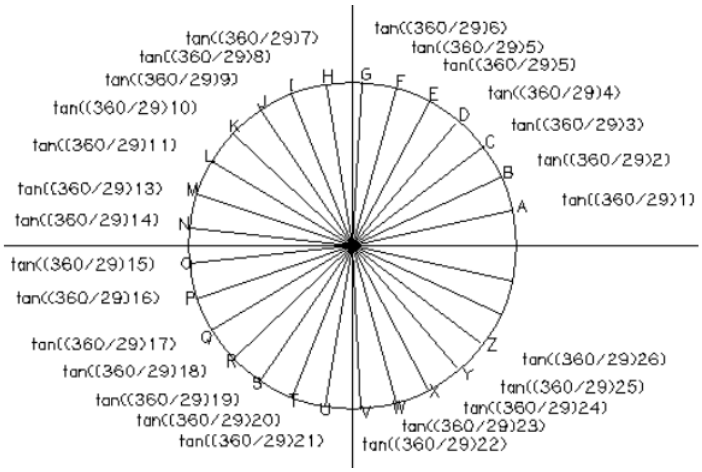

Fig. 1: Representation of the characters over the prime divisions of a circle located at the roots of unity ($p = 29$).

The proposed algorithm encrypts each character by the set of digits from the irrational tangent value located between the M^{th} and N^{th} decimal positions. Additionally, we add a layer of encryption by rotating the set of characters while conserving the irrationality of the tangent values. Specifically, we show that by choosing a rotation angle with a rational tangent, the tangent values associated with the rotated characters will still be irrational.

The private key of the proposed encryption consists of the prime number p, the rotation angle θ, and the integers M and N. At the receiver, the decryption will be a straightforward matching of the received encrypted characters to the assigned characters on the circle. We show that the blind decryption or a hacker attack of the proposed algorithm will require $p!$ number of operations, which is prohibited for large values of primes p.

The paper is organized as follows: in Section 2, we describe the encryption algorithm. Specifically, we prove the two fundamental results of this encryption: (a) the tangent values of the prime roots of unity are irrational numbers, and (b) the irrationality property is preserved if we rotate the unit circle by an angle with a rational tangent. We also provide examples of the encryption and decryption procedures. Section 3 discusses possible attacks on the proposed algorithm, and shows that a brute force attack would require $p!$ operations. Finally, Section 4 summarizes the main results of the paper, proposes future directions and provides possible applications of the proposed encryption. Throughout the paper, we provide reference to known results and limit the presentation of proofs to new contributions. The proofs of original results are provided in the Appendix.

2. The Encryption Algorithm

We consider the prime roots of unity, which are distributed over the unit circle, as in Fig. 1. The proposed encryption algorithm relies on the fact that the tangent values of the prime roots of unity are irrational. The following proposition proves this fundamental result.

Proposition 1: *Let $p \geq 3$ be a prime number. Consider the non-zero angles of the p^{th} roots of unity given by $\theta_k = \frac{2\pi k}{p}$, $k = 1, ..., p-1$. Then we have:*

$$\tan\left(\frac{2\pi k}{p}\right) \in \mathrm{Q},\ k = 1, ..., p-1 \tag{1}$$

where tan *is the tangent function and* Q *is the set of rational numbers. That is, the tangent values of the non-zero angles associated with the prime roots of unity are irrational numbers*.

The irrationality property provides for an infinite number of digits, which can be used to associate characters with numbers in a seemingly random fashion. We further add another layer of encryption by rotating the unit circle by an angle θ in such a way to keep the irrationality property of the tangent values, as detailed in the following proposition.

Proposition 2: *Let $p \geq 3$ be a prime number and β an angle of the form of an arctangent of a rational number, i.e.,* $\beta = \arctan(\frac{r}{q})$, *where* $r, q \in \mathrm{N}$. *Consider the angles of the* p^{th} *roots of unity given by* $\theta_k = \frac{2\pi k}{p}$, $k = 1, ..., p - 1$. *Then, we have:*

$$\tan(\frac{2\pi k}{p} + \beta) \notin \mathrm{Q}, \; k = 1, ..., p - 1 \tag{2}$$

Propositions 1 and 2 provide the theoretical backbone of the proposed encryption algorithm summarized below.

2.1. Encryption algorithm

1. Select a prime number p such that $p > K$, where K is the number of characters to be encrypted.
2. Select the angle of rotation β as the arctangent of a rational number, i.e., $\beta = \arctan(\frac{a}{b})$, where a and b are integers, and such that all tangent values $\tan(\frac{2\pi k}{p} + \beta)$, $k = 1, ..., p - 1$ are distinct.
3. Calculate the tangent values of the rotated prime roots of unity angles as follows: $\tan(\frac{2\pi k}{p} + \beta)$, $k = 1, ..., K$.
4. Select two positive integers M and N such that $N > M$. Each character is encoded by the digits of the irrational number, computed in step 3, between the M^{th} and N^{th} position at the right of the decimal.

The private key of this encryption system is provided by the prime number p, the rotation angle β, and the integers M and N. Given the private key (p, β, M, N) the decryption process is accomplished according to the following steps.

2.2. Decryption algorithm

1. Compute the tangent values $\tan(\frac{2\pi k}{p} + \beta)$, $k = 1, ..., K$.
2. Select the digits between the M^{th} and N^{th} decimal points.
3. Match the received digits with the characters that are associated with them.

2.3. Example

The following example illustrates the encryption algorithm. Let $p = 5$, $M = 5$, $N = 7$, and $\beta = \arctan(\frac{1247}{18234})$. Consider the character set $\{A, B, C, D\}$. Then, we have:

$$\tan(\frac{2\pi}{5} + \arctan(\frac{1247}{18234})) \approx 3.98478529$$
$$\tan(\frac{4\pi}{5} + \arctan(\frac{1247}{18234})) \approx -0.62699986$$
$$\tan(\frac{6\pi}{5} + \arctan(\frac{1247}{18234})) \approx 0.83649441$$
$$\tan(\frac{8\pi}{5} + \arctan(\frac{1247}{18234})) \approx -2.48603667$$

The encrypted values of the characters are then given by $A = 852$, $B = 998$, $C = 944$, $D = 366$. Assume that we wish to securely transmit the message "*ADC*", then we transmit the sequence "852366944". At the receiver, the message is easily decrypted given the private key ($p = 5$, $\beta = \arctan(\frac{1247}{18234})$, $M = 5$, $N = 7$).

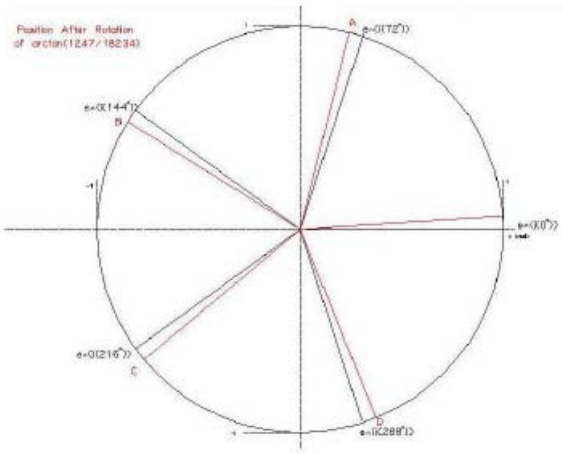

Fig. 2: Representation of the rotated four characters in Example 2.3.

3. Attacks on the Proposed Encryption

In this section, we discuss some of the possible attacks on the proposed algorithm. A random mapping attack requires $p!$ operations. Therefore, by choosing p very large (as in the choice of m in RSA encryption), the random mapping attack can be computationally prohibitive. Observe that p can be much larger than the number of characters to be encrypted, i.e., $p >> K$. In this case, the other $p - K$ tangent values would correspond to dummy or fake characters.

Another attack strategy is to decipher the first M digits in each sequence knowing the digits between the M^{th} and N^{th} positions (which are the transmitted digits). For each character, there are 10^M numerical sequences of length M. Therefore, there are 10^{Mp} possible sequences of length M for all characters. For the two attacks to be comparable in terms of computational complexity, we must have $p! \approx 10^{Mp}$ or $M \approx \log_{10}(p)$. On the other hand, we must have $10^{N-M} \geq p$ in order to guarantee that the tangent values between the M^{th} and N^{th} decimal positions are distinct. If we choose $10^{N-M} \approx 10p$, then, $N - M \approx \log_{10}(p)$. Hence, good choices of the parameters M and N are $M \approx \log_{10}(p)$ and $N \approx 2M \approx 2\log_{10}(p)$.

4. Conclusion

We presented a new encryption algorithm based on the prime roots of unity. We proved that the tangent values of the prime roots of unity are irrational numbers. Furthermore, rotation of the roots by any angle, with a rational tangent, preserves the irrationality of the tangent values. We encrypt the characters by choosing a subsequence of the decimal representation of the irrational number. Given that pseudo-random sequences can be generated from expansions of irrational numbers, the proposed algorithm applies pseudo-random sequences to encrypt the characters. A brute force attack on the cryptosystem results in $p!$ operations for a prime number p. Therefore, choosing a large prime number renders such attacks computationally obsolete. The proposed algorithm can be employed for secure communication, i.e., encryption of voice and text.

5. Appendix

Proof 1 (Proof of Proposition 1): *Consider the p^{th} roots of unity, $z = x + iy = e^{i\frac{2\pi k}{p}}$, $k = 1, ..., p - 1$, which correspond to non-zero angles $\theta = \frac{2\pi k}{p}$, $k = 1, ..., p - 1$. Then $\tan(\theta) = \frac{y}{x} = \alpha$. We have*

$$z^p = 1 \Leftrightarrow (x + iy)^p = 1 \Leftrightarrow x^p (1 + i\alpha)^p = 1 \Rightarrow \text{Im}\left\{(1 + i\alpha)^p\right\} = 0, \tag{3}$$

where Im *denotes the imaginary part. From the binomial formula we have*

$$(1+i\alpha)^p = \sum_{k=0}^{p} \binom{p}{k} i^k \alpha^k \tag{4}$$

Therefore,

$$\mathrm{Im}\left\{(1+i\alpha)^p\right\} = \sum_{k=1}^{\frac{p-1}{2}} \binom{p}{2k+1} (-1)^k \alpha^{2k+1} = 0. \tag{5}$$

Since $\alpha = 0$ *is not a solution of Eq. (5) because* $z \neq 1$, *we can divide by* α *and obtain*

$$\sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k+1} (-1)^k \alpha^{2k} = 0. \tag{6}$$

Let us assume that $\alpha \in \mathrm{Q}$ *and write* α *as an irreducible fraction* $\alpha = \frac{s}{q}$, *i.e., the greatest common divisor of* s *and* q *is* 1. *Multiplying Eq. (6) by* q^{p-1}, *we obtain*

$$\sum_{k=0}^{\frac{p-1}{2}} \binom{p}{2k+1} (-1)^k q^{p-1-2k} s^{2k} = 0 \Leftrightarrow \tag{7}$$

$$pq^{p-1} - \binom{p}{3} q^{p-3} s^2 + \ldots + (-1)^{\frac{p-1}{2}} s^{p-1} = 0 \tag{8}$$

Observe that all the terms in Eq. (8), except the last term, are divisible by p. *Since the sum of these integers is zero, the last term must also be divisible by* p. *Therefore,* s^{p-1} *is divisible by* p. *Since* p *is prime*,

s is divisible by p.

In particular, s^{p-1} *is divisible by* p^{p-1}. *Since* $p - 1 \geq 2$, s^{p-1} *is divisible by* p^2. *Observe also that all the terms in the integer-coefficient polynomial in Eq. (8) are divisible by* p *because all the binomial coefficients are divisible by* p, *and, for the last term,* s *is divisible by* p. *Moreover, since all the terms, except the first term, contain* s *and* s *is divisible by* p, *all terms, except the first term, are divisible by* p^2. *Therefore, the first term* pq^{p-1} *must be divisible by* p^2. *Since* p *is prime*,

q is divisible by p.

Since both s *and* q *are divisible by* p, *the fraction* s/q *is not irreducible. This contradicts the original assumption that* $\alpha = \frac{s}{q}$ *is irreducible. We conclude that* $\alpha = \tan(\theta)$ *is irrational.*

Proof 2 (Proof of Proposition 2): *Let* $\theta_k = \frac{2\pi k}{p}$, $k = 1, \ldots, p-1$. *We have*

$$\tan(\theta_k + \beta) = \frac{\tan(\theta_k) + \tan(\beta)}{1 - \tan(\theta_k)\tan(\beta)}. \tag{9}$$

We show that if $\tan(\beta) \in \mathrm{Q}$, *then* $\tan(\theta_k + \beta) \notin \mathrm{Q}$ *for* $k = 1, \ldots, p-1$. *Let* $\tan(\beta) = \frac{r}{q}$, *where* r *and* q *are integers. Then*

$$\tan(\theta_k + \beta) = \frac{\tan(\theta_k) + \frac{r}{q}}{1 - \frac{r}{q}\tan(\theta_k)}. \tag{10}$$

Assume that $\tan(\theta_k + \beta) \in \mathrm{Q}$, *i.e,* $\tan(\theta_k + \beta) = \frac{s}{n}$, *for some integers* s *and* k. *Then, from Eq. (10), we obtain*

$$\frac{s}{n} - \frac{sr}{nq}\tan(\theta_k) = \tan(\theta_k) + \frac{r}{q} \tag{11}$$

$$\Leftrightarrow \left(1+\frac{sr}{nq}\right)\tan(\theta_k)=\frac{s}{n}-\frac{r}{q}. \tag{12}$$

But from Proposition 1, $\tan(\theta_k)\notin \mathrm{Q}$, $k = 1, ..., p-1$. *Therefore, Eq. (12) can only be true if and only if*

$$1+\frac{sr}{nq}=0 \text{ and } \frac{s}{n}=\frac{r}{q} \tag{13}$$

$$\Leftrightarrow \frac{s}{n}=-\frac{q}{r} \text{ and } \frac{s}{n}=\frac{r}{q} \tag{14}$$

$$\Rightarrow \frac{r}{q}=-\frac{q}{r}\Rightarrow r^2=-q^2 : \textit{ impossible.} \tag{15}$$

Therefore, we conclude that $\tan(\theta_k+\beta)\notin \mathrm{Q}$ *when* $\tan(\beta)\in \mathrm{Q}$.

6. References

[1] R. L. Rivest, A. Shamir, and L. Adelman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. 1978, **21**: 120-126.

[2] S. J. Aboud, M. A. Al-Fayoumi, M. Al-Fayoumi, and H. Jabbar. An efficient RSA public key encryption scheme. *Proc. of International Conference on Information Technology*. 2008, pp. 127-130.

[3] A. Boldyreva, H. Imai, and K. Kobara. How to strengthen the security of RSA-OAEP. *IEEE Transactions on Information Theory*. 2010, **56** (11): 5876-5886.

[4] S. Hung-Min, W. Mu-En, T. Wei-Chi, and M. J. Hinek. Dual RSA and its security analysis. *IEEE Transactions on Information Theory*. 2007, **53** (8): 2922-2933.

[5] H. Ghodosi, C. Charnes, J. Pieprzyk, and R. Safavi-Naini. Pseudorandom sequences obtained from expansions of irrational numbers. *Proc. of Cryptography Policy and Algorithms Conference*. 1995, pp.165-177.