Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44) 12** : 1–8.
ISSN-0037-8712
doi:10.5269/bspm.82035

Number Theory and Applications in Cryptography

Sattar Abd Karabt and Ahmed Hameed Kamil

ABSTRACT: The paper gives an outline of some number theory concepts and shows how those concepts are used in modern information security systems. For example, the Diffie-Hellman Protocol for the generation of pair keys and the RSA and El Gamal public key encryption algorithms are some of the most well-known protocols and methods. In general, one of the most often used applications of number theory in cryptography is the generalized Euclid technique. It is given algorithms, and details on the RSA and ElGamal signature systems are presented. A simplified pairing situation in the explicit rule of reciprocity is used in the bilinear transformation-based approach for electronic signatures.

Keywords: Number theory, cryptography protocols, public key cryptographic algorithms, signature, bilinear transformation.

Contents

1. Introduction

One of my friends, who graduated from Bagdad University, asked me once: "Well, what are you you do in your mathematics, because we went through all of Higher Mathematics at the institute." In this work, we will try to clarify this misconception of so many people not only in our country [6]. Let's try to do this using the example of number theory and cryptography. Number theory is a very ancient science, which has now grown into the direction of "Arithmetic geometry". But even the oldest fundamental results of this science only in our time find application in the now very popular applied science - cryptography [5]. We will show this using the example of Euler's theorem from number theory, which was proved in the middle of the 18th century and found its application in the first modern method of cryptography, RSA, created in 1978 [9]. In the second part of the work, it will be described how the final solution of Hilbert's problem 9 in 1978 [2] gave in 2003 a new way of electronic signature.

2020 *Mathematics Subject Classification:* 11T71, 94A60.
Submitted February 17, 2026. Published June 08, 2026.

2. Number Theory

2.1. Euler's Function

We define the Euler function $\phi(m)$ for an integer $m > 1$ as follows.
Consider all there maunders when dividing by the number $m : 0, 1, 2, ..., m-1$ and count the number of coprime with m, residues. This number will be called the Euler function. Let's consider two special cases:

- If p is a prime number, then it is easy to see that $\phi(p) = p - 1$.
- If p and q are two distinct primes, then $\phi(pq) = (p-1)(q-1)$.

2.2. Euler's Theorem

Theorem 2.1 *[1]: Let a and m be coprime numbers, then the comparison*

$$a^{\phi(m)} = 1(mod\, m). \tag{2.1}$$

3. Extended Euclid's Algorithm

To understand the operations performed in cryptographic transformations, one of the most commonly used tools is the extended Euclid algorithm for finding the multiplicative inverse modulo of some integer. It should be noted that in the general case the application of this algorithm is much wider and affects not only cryptographic transformations but also [13], for example, the theory of algebraic coding. However, here we will focus only on the possibilities of this remarkable algorithm for our purposes, namely, the calculation of the number x inverse to the multiplication of the number y modulo the integer p.

$$x : x.y \equiv 1(mod\, p)$$

A necessary condition for finding such an x is obviously that y and p are mutually prime. The extended Euclidean algorithm uses auxiliary elements u connected by the recursive formula

$$u_{i+1} = (q_1.u_i) + u_{i-1}$$

where $u_{-1} = 0, u_0 = 1$, and q_i is the quotient obtained at the $i - th$ step of the algorithm.
We now give the sequence of steps of the algorithm:

Step 1. $p = y.q_1 + r_1, u_1 = (q_1.u_0) + u_{-1}$,

where q_1 and r_1 is the quotient and the remainder of p divided by y, respectively.

Step 2. $y = r_1.q_2 + r_2, u_2 = q_2.u_1 + u_0$

Step 3. $r_1 = r_2.q_3 + r_3, u_3 = q_3.u_2 + u_1$

Step i. $r_{i-2} = r_{i-1}.q_i + r_i, u_i = q_i.u_{i-1} + u_{i-2}$

$\vdots$

Step ℓ. $r_{\ell-2} = r_{\ell-1}.q_\ell + 1, u_\ell = q_\ell.u_{\ell-1} + u_{\ell-2}$

This is the last step of the algorithm, since the remainder obtained at this step is equal to 1- the greatest common divisor of the numbers p and y. The desired x value is determined as follows:

$$x \equiv (-1)^\ell.u_\ell\, mod\, p.$$

4. Applications in Cryptography

4.1. Asymmetric cryptography

The history of the creation of cryptographic algorithms is no less mysterious and secret than the algorithms themselves [7]. The idea of transmitting secret information over an insecure channel was originally proposed by James H. Ellis in 1970 [12]. Then Ellis, Cocks and Williamson in 1973 [11] proposed the idea of the RSA algorithm, but the result was classified by Government Communications Headquarters (Great Britain) and only on December 18, 1997, Clifford Cocks announced it, making it public. Unfortunately James Ellis died on 25 November 1997 a month before the public announcement of this fact [4]. In 2010, Malcolm Williamson, Clifford Cocks, and James Ellis received the prestigious IEEE Milestone Award for their development of public key cryptography [3]. Consider here what algorithm was proposed by these three Britons.

4.1.1. ***WCE algorithm.*** Two large prime numbers p and q are chosen as the secret key. The public key is their product $N = p.q$ The message m must satisfy the following restrictions: it is a positive integer, mN. In order to encrypt the message, it must be raised to the power of the public key N and the result modulo N (that is, calculate the remainder of the division).

$$e = m^n \,(mod\, N) \tag{4.1}$$

Thus, knowledge of only the public key is sufficient for encryption. At the same time, we note here that the public key in the WCE algorithm is a single number N, which is the product of two secret prime numbers p and q such that

$$(p, (q-1)) = 1, (q, (p-1)) = 1.$$

In order to decrypt the message, knowledge of the secret key is required. Initially, the Euler function $\phi(N) = (p-1)(q-1)$ is found and an auxiliary number is calculated with

$$c = N \,(mod\, \phi(N).)$$

Then the secret key d is calculated

$$d.c = 1 \,(mod\, \phi(N)).$$

For this, the extended Euclid algorithm is used. It should be noted here that a very important property is automatically fulfilled for the correct operation of the extended Euclidean algorithm. Namely, the greatest common divisor of the numbers N and $\phi(N)$ is equal to 1. And, finally, the encrypted message e is raised to the power of d.

$$m = e^d = m^{cd} = m^{1\,(mod\,\phi(N))} = m \,(mod\, N).$$

and now let's look at the official, most common, version of the appearance of asymmetric cryptography.

4.1.2. ***Diffie-Hellman protocol.*** In 1976, the Americans Whitfield Diffie and Martin Hellman published an article "New directions in cryptography" [8] in the IEEE Transaction on Information Theory magazine, in which they described an encryption scheme without exchanging a secret key over an open channel. The main idea underlying the proposed protocol was the use of the discrete logarithm problem. That is, the absence of an effective algorithm for calculating the number x with known prime number p, and integers a and b.

$$a = b^x \,(mod(p))$$

What is this protocol, published over 40 years ago and still effectively used in a huge number of practical applications that provide a secure channel for any two devices that did not have any information about each other before 0 to a friend and using a communication channel freely listened to by everyone to develop a secret key.

The first step of the protocol is the choice by the parties in an open discussion of a pair of numbers: a large prime number p and a b-primitive root of 1 modulo p. At the second step, each of the participants in the protocol chooses their own secret number. Accordingly x, y.

$$1 < x < p-1, 1 < y < p-1.$$

To exchange over an open, monitored channel, the participants calculate the numbers

$$a = b^x \, (mod(p))$$

and

$$c = b^x \, (mod(p))$$

respectively. After receiving these values, the participants in the protocol can calculate the shared pair key K.

$$K = a^y = c^x = b^{xy} \, (mod(p).) \tag{4.2}$$

4.1.3. ***RSA encryption algorithm.*** In 1978, Ronald Rivest, Adi Shamir and Leonard Adleman patented and published their algorithm, which was later called RSA [9]. In the same issue of the journal, the famous mathematician and scientist Martin Gardner, with the consent of the authors of the algorithm, published a mathematical problem called RSA-129. In the condition of the problem, he indicated two numbers n and e-the public key and the cipher text. The length of the number n was 129 decimal places, and the number $e = 1007$. A bonus of \$100 was supposed to be awarded for deciphering the text. The cipher was cracked after 17 years - about 600 people joined the network and with the efforts of 1600 computers in six months they were able to read the phrase in 1995:

"The Magic Words are Squesmish Ossifrage"

Main steps of the RSA algorithm Secret key selection and public key calculation:

Step 1. We choose large prime numbers p and q with a close number of digits and calculate $N = pq$.

Step 2. Calculate $\phi(N) = (p-1)(q-1)$.

Step 3. Randomly.
choose a number c coprime to $\phi(N)$.

Step 4. Using the extended Euclid algorithm, calculate the number d with

$$c.d \equiv 1 \, (mod \, \phi(N).)$$

Definition 4.1 *The number d is a secret key, as are the numbers p and q.*

Definition 4.2 *A pair (c, N) is a public key that is distributed openly. Encryption of messages using the public key. The message can be any positive integer m not exceeding N. The public key is used for encryption:*

$$e = m^c \, (mod(N).)$$

Decryption using a private key. We raise the number e to the power d and look for the remainder of the number e^d when divided by N. This will be m

$$e^d = m^{cd} \equiv m^{1+k.\phi(n)} \equiv m + e.N \equiv m \, (mod(N).)$$

Remark 4.1 *If the number N has 100 digits, then there are at least 4.10^{42} prime numbers that can divide the number N. If the computer performs 1 million operations per second, then it will take about 10^{35} years to calculate $\phi(N)$.*

Remark 4.2 *The RSA algorithm used by Gardner for his contest used 64 and 65 digit primes.*

Remark 4.3 *Now for the algorithm, RSA uses 150-digit primes.*

4.2. El-Gamal algorithm

The main steps of the El-Gamal algorithm In 1985, in the journal IEEE Transactions on Information Theorv [10], Taher El-Gamal proposed an encryption algorithm using the ideas of the Diffie-Hellman protocol. Unlike previous authors, El-Gamal did not patent his scheme and, in many respects, it was precisely because of this that it was used as the basis for national standards in most countries (Russia, USA, Europe, etc.).
Secret key selection and public key calculation:

Step 1. We choose a large prime number p and q is a primitive root of unity modulo p.

Step 2. Randomly choose a number $c, 1 < c < p - 1$.

Step 3. Calculate $b = q^c \, (mod(pp))$.

Definition 4.3 *The number c is the secret key.*

Definition 4.4 *A triple of numbers (p, q, b) is a public key that is distributed openly.*

"Encryption of messages using the public key"

The message can be any positive integer m not exceeding N. The encryption uses the public key and a random number $r, 1 < r < p - 1$:

$$e = m.b^r \, (mod(p).)$$

Definition 4.5 *An encrypted message is represented by a pair of numbers:*

$$(e, f) \equiv (q^r \, (mod(p)).)$$

Decryption using a private key. We raise the number f to the power c and get $bz \, mod(p)$.

$$f^c = q^{rc} = q^{cr} = b^r \, mod(p).$$

Using the extended Euclidean algorithm, we find the multiplicatively inverse of d to b^r modulo p.

$$d.b^r = 1 \, (mod \, (p).)$$

Now it remains to multiply the first of the pair of numbers presented in the encrypted message and we will get the original message.

$$e.d \equiv t.b^r.d \equiv m.1 = m \, (mod \, (p).)$$

4.3. RSA electronic signature

Using the notation introduced earlier, we describe the stages of calculating an electronic signature and its verification, assuming that for a message m the value of the hash function is equal to h and $h < N$. Then the signature s is calculated as follows:

$$s = h^d \, (mod \, (N).)$$

After calculating the electronic signature, the stored or transmitted information is a pair a message and a signature (m, s). It is not difficult to see that the signature algorithm for RSA is the same as the decryption algorithm and naturally requires a secret key.
In order to check the correctness of the electronic signature s, that is, to check whether the original document t is not distorted and whether it is really signed by a specific person who has the public key (c, N), you must perform the following steps:

- Calculate the hash function from the checked message $\acute{m}, \acute{h} = Hash(\acute{m})$.
- Check whether the equality $s^c = \acute{h} \, mod \, (N)$ is satisfied.

Obviously, only the public key (c, N) is needed to perform these operations.

4.4. Electronic signature of El-Gamal

The El-Gamal signature is implemented much more complicated and, most importantly, requires the use of a random number, which, on the one hand, makes it difficult to calculate it, and on the other hand, makes it more secure, since the same message signed by the same user will have a different signature each time.
In the presence of a secret key c and a public key $r(p, q, b)$, we also need a random positive integer r such that $1 < r < p - 1$ and the greatest common divisor $rwp - 1$ is equal to 1.
The electronic signature s for the message m, with the hash function h is calculated from the relation

$$h \equiv r.s + f.s\,(mod\,(p-1).)$$

Where

$$f = q^r\,(mod(p).)$$

It is not difficult to see that here again it is necessary to find the multiplicative inverse to $rmodulop - 1$, and this can be done only in the case when

$$(r, (p-1)) = 1.$$

The signature in the El-Gamal system, as well as in encryption, is two numbers (s, f). Message $\acute{m}$, signature (s, f) and the user's public key are required to check the integrity of the message and ownership of the signature. If there were no distortions, then there are

$$\acute{m} = m, \acute{h} = Hash(\acute{m}) = Hash(m) = h$$

and the signature was computed by the user with the public key (p, q, b) and its corresponding private key with then a comparison will be made

$$q^h \equiv f^s.b^f \equiv q^{r.s}.q^{c.f} \equiv q^{r.s+c.f} \equiv q^{h+e.(p-1)} = q^h\,(mod(p).)$$

4.5. Electronic signature on bilinear transformation

The method for creating an electronic signature, which will now be proposed, uses a simplified form of pairing in the explicit reciprocity law obtained by C.B Vostokov in [2].
The set of integers coprime with p:

$$z^p = \{a \in Z | g.c.d.\, ap = 1\}.$$

It is clear from the properties of coprime numbers that multiplication leaves numbers from (z^p) in the same set. LetN^+ be the set of natural numbers with the operation of addition. Set the pairing

$$\begin{aligned} <,> p : Z^{(p)}X &= N^+ \to Z\,(mod(p)) \\ < a, n > &= \ell(a)n\,(mod(p)) \\ I(a) &= \frac{\log a^{p-1}}{p} \\ \log(1+x) &= x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots . \end{aligned}$$

Definition 4.6 *The number a is called the Wieferich number if*

$$a^{p-1} \equiv 1\,(mod(p^2)).$$

Otherwise, the case will be called anti-wiferich.

Lemma 4.1 *The pairing $\{,\}_p$ is bilinear, that is,*

$$\begin{aligned} < ad, n > &= < a, n >_p + < b, n >_p, \textit{for any } a \textit{ and } b \textit{ from } z^p; \\ < a, n+m > &= < a, n >_p + < a, m >_p \textit{ for any } n \textit{ and } m \textit{ from } N^+. \end{aligned}$$

Moreover, this pairing is non-degenerate for an anti-Wieferich number a, i.e. for such a there exists n from N^+ such that h, then $< a, n >_p = 1\,(mod\, p)$.

Proof:

- Bilinearity in the second argument is obvious, and in the first argument it follows from the properties of the logarithm.
- Non-degeneracy. Let a be an anti-Wieferich number. Then

$$\frac{a^{p-1}-p}{p}$$

$$L(a)=\frac{\log(a^{p-1})}{p}=\frac{\log(1+\frac{a^{p-1}-1}{p}p)}{p}=\frac{\frac{a^{p-1}}{p}p}{p}-\frac{(\frac{a^{p-1}}{p}p)^2}{2p}+\cdot=\frac{a^{p-1}-1}{p}$$

not divisible by p. Then we can take as n such a number that the pairing $< a,n >_p$ becomes equal to $1\,mod\,(p)$.
Indeed, since the $g.c.d\,l(a)_p=1$
then there are integers x and y such that $l(a)x+py=1$. Replacing, if necessary,x by $\acute{x}=x+pk$, and y by $\acute{y}=y-l(a)k$, we obtain, for suitable k, that $\acute{x}$ is a natural number. □

4.5.1. ***Signature generation.*** Alice is a confidant (arbiter). It chooses a large prime number p, an antiwieferich number coprime with it a from and a natural number n from N such that the congruence. Let x be a random number such that $1<x<p$ and s be the solution to the congruence $sx\equiv n\,(mod\,p)$.

Definition 4.7 The set (a,x,n) is a secret key.

Let $M=\{m_1,m_2,\cdot,m_k\}$ be information (message). In cryptography, a function is defined, called a hash function, which is uniquely given by the information M. Let's find the remainder when dividing a^{hx} by p^2.

$$r=a^{hx}\,(mod\,p^2), 0<r<p^2$$

The signed message has the form $\Pi=(M,\Gamma<s<h)$. The recipient Bob must check the signature, that is, check the validity of the comparison.

$$\frac{r^{p-1}-1}{p}.s\equiv h\,(mod\,p.) \tag{4.3}$$

that is, the remainder $\frac{r^{p-1}-1}{p}.s$ when divided by p must be equal to ha.

Lemma 4.2 *If the signature is correct, then the comparison (4.3)is satisfied.*

Proof: Let us calculate the pairing $< r,s >_p$. We have

$$< r,s >_p\equiv l(r).s\equiv\frac{\log(1+\frac{r^{p-1}-1}{p})}{p}.s=\frac{r^{p-1}-1}{p}.s\equiv h\,(mod\,p)$$

Indeed, since $r=a^{hx}\,(mod\,p^2)$, then

$$< r,s >_p=< a^{hx},s >_p\equiv x<a^h,s >_p\equiv< a^h,sx >_p\equiv h<a,n >_p\equiv h\,(mod\,p)$$

□

Lemma 4.3 *Signature* Π *satisfies the requirements for a signature, that is 1. no one except Alice can sign a message with her signature; 2. in the event of a conflict between Alice and Bob, they turn to third parties, and the judge checks the authenticity of the signature after presenting him with numbers* (a,x,n).

5. Conclusion

In this paper, cryptographic primitives of encryption and signature are considered using the basic concepts of number theory. An electronic signature algorithm based on a bilinear transformation using a simplified form of pairing in an explicit reciprocity law, described by C.B. Vostokov in work [2], where the final solution of the 9th Hilbert problem.

References

1. Burton, David. Ebook:*Elementary number theory.* McGraw Hill, 2010.
2. Vostokov, S. V. *vna forma zakona vzaimnosti.— Izv.* AN SSSR. Ser. matem 42 (1978): 1287-1320.
3. W. Stallings,*Cryptography and Network Security: Principles and Practice*,4th ed.Upper Saddle River, NJ, USA: Pearson, 2005.
4. A. Buchshtab,, *Number Theory*, Moscow (1960).
5. S.V. Vostokov, O.V. Demchenko,, *Gil'bert's explicit pairing formula for formal groups of Honda*, Zap. scientific. seven. POMI, 272, pp. 86-128,2000
6. A. P. U. Siahaan, E. Elviwani, and B.Oktaviana,*Comparative analysis of RSA and ElGamal cryptographic public-key algorithms,* in Proc. Joint Workshop KO2PI , 1st Int. Conf. on Advance , Scientific Innovation,2018.
7. R.L. Rivest, A. Shamir, L. Adleman.*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.* MIT Laboratory for computer Science and Department of Mathematics. Volume 21, number 2.(1978).
8. N. Koblik, *Course of Number Theory and Cryptography*, Moscow, ed. TVP,P.P254, 2001.
9. Chey Cobb,*Cryptography for Dummies*, 2004.
10. Dan Boneh and Xavier Boyen. *Short signatures without random oracles.* In Christian Cachin and Jan Camenisch, editors, EUROCRYPT 2004, volume 3027 of LNCS, pages 56-73. Springer, pMay 2004.
11. T. El-Gamal.*A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms.* In(1985).
12. Blakley G.R., Chaum D. (eds) *Advances in Cryptology.* CRYPTO 1984.
13. D. Kahn,, *Codebreakers, Centerpolygraph,* P.P 480,2000.

Ahmed Hameed Kamil,
Department of Mathematics,
College of Computer Science and Mathematics,
University of Thi-Qar,
Iraq.
E-mail address: ahmedhameed1992@utq.edu.iq