Applications of Number Theory in Cryptography

Prof.dr. Ferucio Laurențiu Țiplea

Spring 2022

Department of Computer Science
“Alexandru Ioan Cuza” University of Iași
Iași 700506, Romania

e-mail: ferucio.tiplea@uaic.ro

Outline

Introduction to cryptography

Factorization and Euler's function

Applications of the CRT

Applications of the Jacobi symbol

Reading and exercise guide

Introduction

Introduction to cryptography

- Cryptography is the field concerned with techniques for securing information, particularly in communications;
- Cryptography focuses on the following main paradigms:
  - Privacy/confidentiality – ensuring that no one can read the message except the intended receiver;
  - Authentication – the process of proving one's identity (the primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak);
  - Integrity – assuring the receiver that the received message has not been altered in any way from the original.

Applications of cryptography

- Computer and information security: cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.
- e-commerce, e-payment, e-voting, e-auction, e-lottery, and e-gambling schemes, are all based on cryptographic (security) protocols.

Examples of software tools that havily rely on cryptographic techniques: IPsec, SSL & TLS, DNSsec, S/MIME, SET etc.

Cryptographic primitives

Crypto primitives:

1. Encryption schemes (ciphers)
2. Digital signature schemes
3. Hash functions
4. Message authentication code (MAC) schemes
5. Secret sharing schemes
6. and more ...

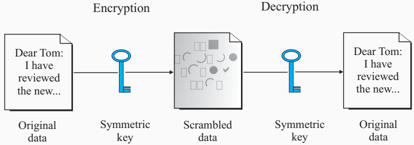
Basic elements of a cryptographic primitive:

1. A message space
2. A key space
3. An output space (of ciphertexts, message digests and so on)
4. Algorithms (for encryption, decryption, hashing, signing and so on)

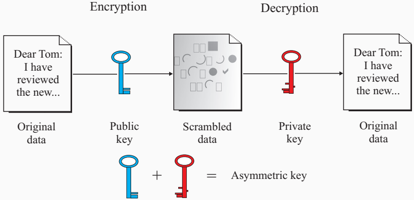
Two classes of cryptographic primitives

Illustration on ciphers:

- Symmetric (private-key, single-key) ciphers – encryptions and decryptions are performed by the same key



- Asymmetric (public-key) ciphers – encryptions are performed by a public-key, while decryptions are performed by a corresponding private key



Factorization and Euler's function

The RSA cipher

The RSA cipher, proposed in 1977 by Ronald Rivest, Adi Shamir, and Leonard Adleman is one of the most prominent public-key ciphers that is still secure and in use.

Key generation: public key: (n, e), where

$n = pq$, p and q distinct primes

$e \in \mathbb{Z}^*_{\phi(n)}$

private key: (p, q, d), where

$ed \equiv 1 \bmod \phi(n)$

Encryption of $x \in \mathbb{Z}_n$: output $c = x^e \bmod n \bmod n$

Decryption of $c \in \mathbb{Z}_n$: output $x = c^d \bmod n$

Correctness: $(x^e)^d \equiv x \bmod n$, for all $x \in \mathbb{Z}_n$ Prove it!

The RSA cipher

Example 1 (With artificially small parameters)

Let $p = 61$ and $q = 53$. Then:

- $n = pq = 3233$ and $\phi(n) = 3120$;
- If we chose $e = 17$, then d can be computed with the extended Euclidean algorithm. We obtain $d = e^{-1}$ *mod* $3120 = 2753$;
- $n = 3233$ and $e = 17$ are public parameters; p, q, and d private;

Let $x = 123$ be a plaintext. The cryptotext is

$$c = 123^{17} \textit{ mod } 3233 = 855.$$

In order to decrypt y we compute

$$855^{2753} \textit{ mod } 3233 = 123.$$

Security of the RSA cipher

Security issues:

- If p or q is recovered (e.g., by factoring n in reasonable time), then the system is completely broken;
- If $\phi(n)$ can be computed in reasonable time, then the system is completely broken;
- If d can be easily computed from n and e, then the system is completely broken.

In practice:

- p and q are 512-bit primes (or even larger);
- e is small (fast encryption) but chosen such that $d > \sqrt[4]{n}$ (otherwise, an efficient attack can be mounted).

For more details visit http://www.rsasecurity.com/.

Digital signatures

Public key cryptography solves another problem crucial to e-commerce and Internet cyber relationship: it lets you emulate written signatures. This use of the public-key is called digital signature.

A digital signature must provide:

- authenticity and integrity. That is, it must be “impossible” for anyone who does not have access to the secret key to forge (x, s) (x is the original data and s is its associated signature);
- non-repudiation. That is, it must be impossible for the legitimate signer to repudiate his own signature.

Signing (encrypting with a private key) is extremely slow, so you usually add a time-saving (and space-saving) step before you encrypt messages. It is called message digesting or hashing.

Digital signatures from public-key ciphers

Public-key ciphers may be used to produce digital signatures:

- Assume that K_e is A's public key and K_d is A's private key and, moreover, $e_{K_e}(d_{K_d}(x)) = x$;
- Then, the decryption of a message x by K_d is the digital signature associated to x. It can be verified by K_e:

  $$x \overset{?}{=} e_{K_e}(d_{K_d}(x)).$$

  Therefore, in such a case, K_d is used to sign messages (it will be secret) and K_e is used to verify signatures (it will be public).

The RSA signature is obtained from the RSA public-key cipher.

The RSA digital signature

Example 2 (With artificially small parameters)

Let $p = 61$ and $q = 53$. Then:

- $n = pq = 3233$ and $\phi(n) = 3120$;
- If we chose $e = 17$, then d can be computed with the extended Euclidean algorithm. We obtain $d = e^{-1}$ *mod* $3120 = 2753$;
- $n = 3233$ and $e = 17$ are public parameters to verify signatures; p, q, and d are private parameters to sign messages;

Let $x = 123$ be a message. The signature is

$$s = 123^{2753} \ mod \ 3233 = 2746.$$

So, $(123, 2746)$ is the signed message.

In order to verify the signature for $(123, 2746)$ we compute

$$2746^{17} \ mod \ 3233 = 123.$$

Applications of the CRT

Threshold sharing schemes

The Chinese Remainder Theorem (CRT) has numerous applications in various fields of mathematics, computer science, and engineering. We illustrate below an application of it to secret sharing.

A (k,n)-threshold sharing scheme, where $k \leq n$, consists of n parties $P_1, \ldots, P_n$ sharing a secret S such that the following properties hold:

1. each P_i has an information I_i (secret share);
2. knowledge of any k of $I_1, \ldots, I_n$ enables one to find S easily;
3. knowledge of less than k of $I_1, \ldots, I_n$ does not enable one to find S easily.

- Party P_i = people, software/hardware computing device ... Simply denote it by i and refer to it as user or participant;
- Secrets and secret shares are usually viewed as integers.

Goldreich-Ron-Sudan (GRS) scheme

1. Parameter setup: integers t and n such that $0 < t + 1 \leq n$ and sequence of pairwise coprime integers $m_0 < m_1 < \cdots < m_n$. All are public parameters;
2. Secret and share spaces: the secret space is $\mathbb{Z}_{m_0}$ and the share space of the ith participant is $\mathbb{Z}_{m_i}$, for all $1 \leq i \leq n$;
3. Secret sharing: given $s \in \mathbb{Z}_{m_0}$, share it by $s_i = s' \ mod \ m_i$, for all $1 \leq i \leq n$, where s' is the unique solution modulo $m_0 \prod_{i=1}^{t} m_i$ of the system

$$x \equiv r_i \ mod \ m_i, \quad 0 \leq i \leq t$$

   where $r_0 = s$ and r_i is randomly chosen from $\mathbb{Z}_{m_i}$ for all $1 \leq i \leq t$;
4. Secret reconstruction: any $t + 1$ distinct shares $s_{i_1}, \ldots, s_{i_{t+1}}$ can uniquely reconstruct the secret s by computing first the unique solution modulo $\prod_{j=1}^{t+1} m_{i_j}$ of the system

$$x \equiv s_{i_j} \ mod \ m_{i_j}, \quad 1 \leq j \leq t + 1$$

Goldreich-Ron-Sudan (GRS) scheme

Example 3 (With artificially small parameters)

1. Parameter setup: $t = 2$, $n = 5$ and

$$m_0 = 31 < m_1 = 37 < m_2 = 41 < m_3 = 43 < m_4 = 47 < m_5 = 53$$

2. Secret sharing: We choose $s = 13$ for sharing, generate $r_1 = 3$ and $r_2 = 5$, and solve the system

$$x \equiv_{31} 13,\ x \equiv_{37} 3,\ x \equiv_{41} 5$$

We get $s' = 37151$ and then the shares 3, 5, 42, 21, 51

3. Secret reconstruction: Assume that the last 3 participants want to recover the secret s. They solve the system

$$x \equiv_{43} 42,\ x \equiv_{47} 21,\ x \equiv_{53} 51$$

and get 37151. By reducing this modulo 31 they obtain $s = 13$.

Security of the GRS scheme

CRT-based secret sharing schemes can only achieve asymptotic security properties:

- X random variable associated with the secret space $\mathbb{Z}_{m_0}$;
- For $I \subseteq \{1, \ldots, n\}$, Y_I random variable associated to the combined share space $\prod_{i \in I} \mathbb{Z}_{m_i}$;
- Loss of entropy: $\Delta(y_I) = H(X) - H(X|Y_I = y_I)$,, where $y_I \in \prod_{i \in I} \mathbb{Z}_{m_i}$ and H is the entropy;
- Asymptotic perfection: $\Delta(y_I) \to 0$ as $m_0 \to \infty$;
- Information rate of the participant i: $|\mathbb{Z}_{m_i}|/|\mathbb{Z}_{m_0}|$;
- Asymptotic idealness: asymptotic perfection and the information rate of each participant goes to 1 as $m_0 \to \infty$.

Security of the GRS scheme

A sequence $m_0, m_1, \ldots, m_n$ of pairwise co-prime integers is called compact if $m_1 < \cdots < m_n$ and there exists $\theta \in (0, 1)$ such that

$$m_0 - m_0^\theta < m_i < m_0 + m_0^\theta,$$

for all $1 \leq i \leq n$.

Theorem 4

The GRS secret sharing scheme is asymptotically ideal if and only if it is based on compact sequences of co-primes.

For full details see [1, 2].

For applications of secret sharing in security protocols see [3].

Applications of the Jacobi symbol

Cocks' PKE scheme

Key generation: public key: (n, a), where

$n = pq$, p and q distinct primes

$a = r^2 \bmod n$ with $r \leftarrow \mathbb{Z}_n^*$

private key: (p, q, r)

Encryption of $m \in \{-1, 1\}$: $t \leftarrow \mathbb{Z}_n^*$ with $\left(\frac{t}{n}\right) = m$

output $c = t + at^{-1} \bmod n$

Decryption of $c \in \mathbb{Z}_n$: output $m = \left(\frac{c+2r}{n}\right)$

Correctness: $\left(\frac{c+2r}{n}\right) = \left(\frac{t^{-1}(t+r)^2}{n}\right) = \left(\frac{t}{n}\right) = m$

For more details see [4]

Cocks' PKE scheme

Example 5 (With artificially small parameters)

Let $p = 61$ *and* $q = 53$. *Then:*

- $n = pq = 3233$ *and let* $r = 17$. *Then,* $a = 289$*;*
- $n = 3233$ *and* $a = 289$ *are public parameters;* p*,* q*, and* r *secrete;*

Let $m = -1$ *be the message to be encrypted. We choose* $t = 951$*. Remark that* $\left(\frac{951}{3233}\right) = -1 = m$*. Then*

$$c = t + at^{-1} \bmod n = (951 + 289 \cdot 1625) \bmod 3233 = 1791$$

is the ciphertext.

In order to decrypt c *we have to compute*

$$\left(\frac{1791 + 2 \cdot 17}{3233}\right) = \left(\frac{1835}{3233}\right) = -1 = m$$

Security of Cocks' PKE scheme

Security issues:

- If a root of a can be efficiently computed, then the system is completely broken;
- If p or q is recovered (e.g., by factoring n in reasonable time), then the system is completely broken;
- $c \equiv t + at^{-1} \bmod n$ is equivalent to $t^2 - ct + a \equiv 0 \bmod n$, for $t \in \mathbb{Z}_n^*$. When a is a quadratic residue modulo n and c is a ciphertext, the congruence may have one, two, or four roots, and all have the same Jacoby symbol. Therefore, if one root can be efficiently computed, the message can be recovered.

Reading and exercise guide

Reading and exercise guide

It is highly recommended that you do all the exercises marked in red from the slides.

It is recommended that you go through the bibliography materials (which can be found freely on the Internet) to get the best possible picture of the applications of number theory in cryptography.

Number theory is currently the basis of most public-key cryptography techniques.

References

[1] Ferucio Laurențiu Țiplea and Constantin Cătălin Drăgan. A necessary and sufficient condition for the asymptotic idealness of the GRS threshold secret sharing scheme. *Inf. Process. Lett.*, 114(6):299?303, jun 2014.

[2] Constantin Cătălin Drăgan and Ferucio Laurențiu Țiplea. On the asymptotic idealness of the Asmuth-Bloom threshold secret sharing scheme. *Information Sciences*, 463-464:75–85, 2018.

[3] Sorin Iftene. *Secret Sharing Schemes with Applications in Security Protocols*. PhD dissertation, "Alexandru Ioan Cuza" University of Iași, 2007.

[4] Ferucio Laurențiu Țiplea, Sorin Iftene, George Teșeleanu, and Anca-Maria Nica. On the distribution of quadratic residues and non-residues modulo composite integers and applications to cryptography. *Applied Mathematics and Computation*, 372, 2020.