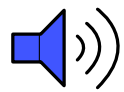
Introduction to Cryptography



Ferucio Laurențiu Țiplea

Department of Computer Science
"Al.I.Cuza" University of Iași
Iași 700506, Romania
e-mail: ferucio.tiplea@uaic.ro

Fall 2020

Outline

Introduction to cryptography

The RSA cryptosystem

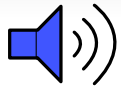
Digital signatures

Secret sharing schemes

Course readings

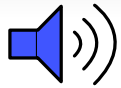
Outline

Introduction to cryptography



- Cryptography is the field concerned with techniques for securing information, particularly in communications;
- Cryptography focuses on the following paradigms:
  - 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);
  - Privacy/confidentiality – ensuring that no one can read the message except the intended receiver;
  - Integrity – assuring the receiver that the received message has not been altered in any way from the original;
  - Non-repudiation – a mechanism to prove that the sender really sent this message.

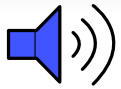
Applications of cryptography



- 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.

History of cryptography



- The oldest forms of cryptography date back to at least Ancient Egypt, when derivations of the standard hieroglyphs of the day were used to communicate;
- Julius Caesar (100-44 BC) used a simple substitution cipher with the normal alphabet (just shifting the letters a fixed amount) in government communications (Caesar cipher);
- Thomas Jefferson, the father of American cryptography, invented a wheel cipher in the 1790's, which would be redeveloped as the Strip Cipher, M-138-A, used by the US Navy during World War II;
- During World War II, two notable machines were employed: the German's Enigma machine, developed by Arthur Scherbius, and the Japanese Purple Machine, developed using techniques first discovered by Herbert O. Yardley;

History of cryptography

- William Frederick Friedman, the father of American cryptanalysis, led a team which broke in 1940 the Japanese Purple Code;
- In the 1970s, Horst Feistel developed a "family" of ciphers, the Feistel ciphers, while working at IBM's Watson Research Laboratory. In 1976, The National Security Agency (NSA) worked with the Feistel ciphers to establish FIPS PUB-46, known today as DES;
- In 1976, Martin Hellman, Whitfield Diffie, and Ralph Merkle, have introduced the concept of public-key cryptography;
- In 1977, Ronald L. Rivest, Adi Shamir and Leonard M. Adleman proposed the first public-key cipher that is still secure and used (it is known as RSA);

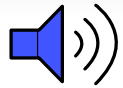
History of cryptography

- The Electronic Frontier Foundation (EFF) built the first unclassified hardware for cracking messages encoded with DES. On July 17, 1998, the EFF DES Cracker was used to recover a DES key in 22 hours. The consensus of the cryptographic community was that DES was not secure;

- In October 2001, after a long searching process, NIST selected the Rijndael cipher, invented by Joan Daemen and Vincent Rijmen, as the Advanced Encryption Standard. The standard was published in November 2002'

- 2002 – : Lots of modern cryptographic techniques developed around cloud security and quantum computing.

Cipher



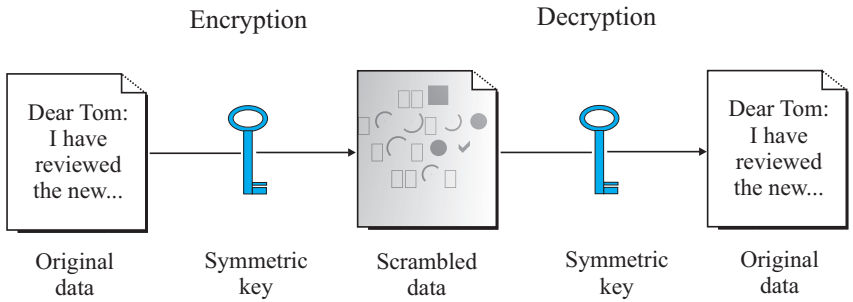
A cipher is an algorithm for converting (encrypting) a message (plaintext) into a ciphertext under the control of a secret key.

Basic elements of a cipher:

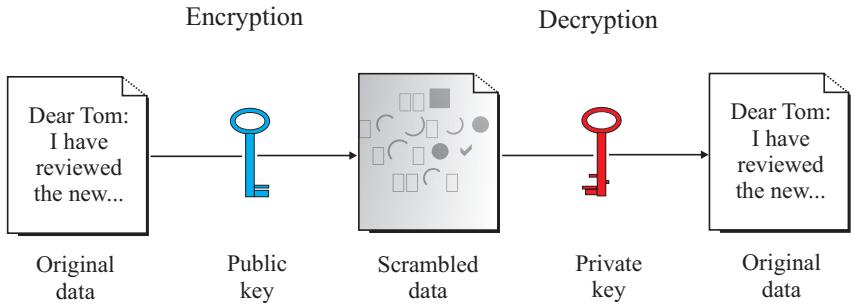
1. A set $\mathcal{K}$ of keys
2. A set $\mathcal{M}$ of messages
3. A set $\mathcal{C}$ of ciphertexts
4. An encryption algorithm $\mathcal{E}$ that converts (encrypts) a message m under a key K into a ciphertext c
5. A decryption algorithm $\mathcal{D}$ that converts back (decrypts) the ciphertext c under some key K' into the message m

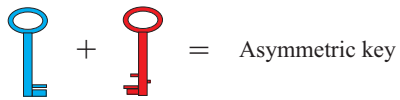
Two classes of ciphers

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

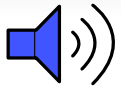


- Asymmetric (public-key) ciphers – encryptions are performed by a (public) key while decryptions are performed by a corresponding private key





Affine cipher



Description 1 (Affine Cipher)

- $\mathcal{M} = \mathcal{C} = V^{\leq \ell}$, *where* $V = \{v_1, \ldots, v_n\}$ *is some given ordered alphabet with* n *letters and* ℓ *is a positive integer;*
- $\mathcal{K} = \{(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n \mid (a, n) = 1\}$
- *For any key* $K = (a, b)$ *and* $m = v_{i_1} \cdots v_{i_t} \in \mathcal{M}$,

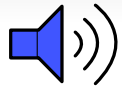
$$e_K(v_{i_1} \cdots v_{i_t}) = v_{j_1} \cdots v_{j_t}$$

where $j_1 = (a \cdot i_1 + b) \bmod n$, *and so on.*
For decryption,

$$d_K(v_{i_1} \cdots v_{i_t}) = v_{j_1} \cdots v_{j_t}$$

where $\mathrm{i}_1 = a^{-1}(\mathrm{j}_1 - b) \bmod n$, *and so on.*

Affine cipher



Example 2

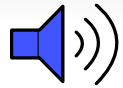
Assume V is the English small letters alphabet, $|V| = 26$. Let $K = (7, 3)$ and the plaintext *hot*. Then,

plaintext	h	o	t
index in V	7	14	19
new index by encryption	0	23	6
ciphertext	a	x	g

Special cases:

1. Shift cipher ($a = 1$)
2. Caesar cipher ($a = 1$ and $b = 3$)

Affine cipher – cryptanalysis



Affine ciphers can be easily broken by exhaustive key search (EKS), also known as brute-force search, which consists of trying every possible key until the right one is found:

$$\text{there are } \phi(n) \times 26 \text{ possible keys}$$

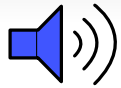
As n is the size of the alphabet, $\phi(n)$ is usually small. For instance, $|V| = 26$ for the English alphabet of the small letters. This leads to $\phi(n) \times 26 = 12 \times 26 = 312$ keys.

Question: How does you know when you have found the correct plaintext ?

Answer: *You know that you have found the plaintext because it looks like a V-language message, or like a data file from a computer application, or like a database in a reasonable format; it looks like something understandable (in some way).*
When you look at a cryptotext file, or a file decrypted with a wrong key, it looks like gibberish.

Outline

The RSA cipher



In 1977, Ronald Rivest, Adi Shamir, and Leonard Adleman, proposed the first public-key cipher that is still secure and in use.

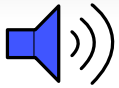
Description 3 (RSA)

- *Let p and q be two distinct primes, and $n = pq$;*
- $\mathcal{M} = \mathcal{C} = \mathbb{Z}_n$;
- $\mathcal{K} = \{(n, p, q, e, d) | e \in \mathbb{Z}^*_{\phi(n)} \ \wedge \ ed \equiv 1 \ mod \ \phi(n)\}$;
- *for any $K = (n, p, q, e, d) \in \mathcal{K}$ and $x, y \in \mathbb{Z}_n$,*

$$e_K(x) = x^e \ mod \ n \ \ and \ \ d_K(y) = y^d \ mod \ n;$$

- *(n, e) is the public key, and (p, q, d) is the secret key.*

The RSA cipher



Example 4 (RSA 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 *secrete;*

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

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

In order to decrypt y *we have to compute*

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

Security of RSA

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.

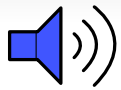
In practice:

- 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: http://www.rsasecurity.com/.

Outline

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 public key technology is called a 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, σ) (x is the original data and σ 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 and message digests

A hash algorithm (function) is an algorithm (function) that, applied to an arbitrary-length input data, produces a fixed-length output data (called a hash value or message digest or fingerprint). Digital signatures are usually applied to message digests.

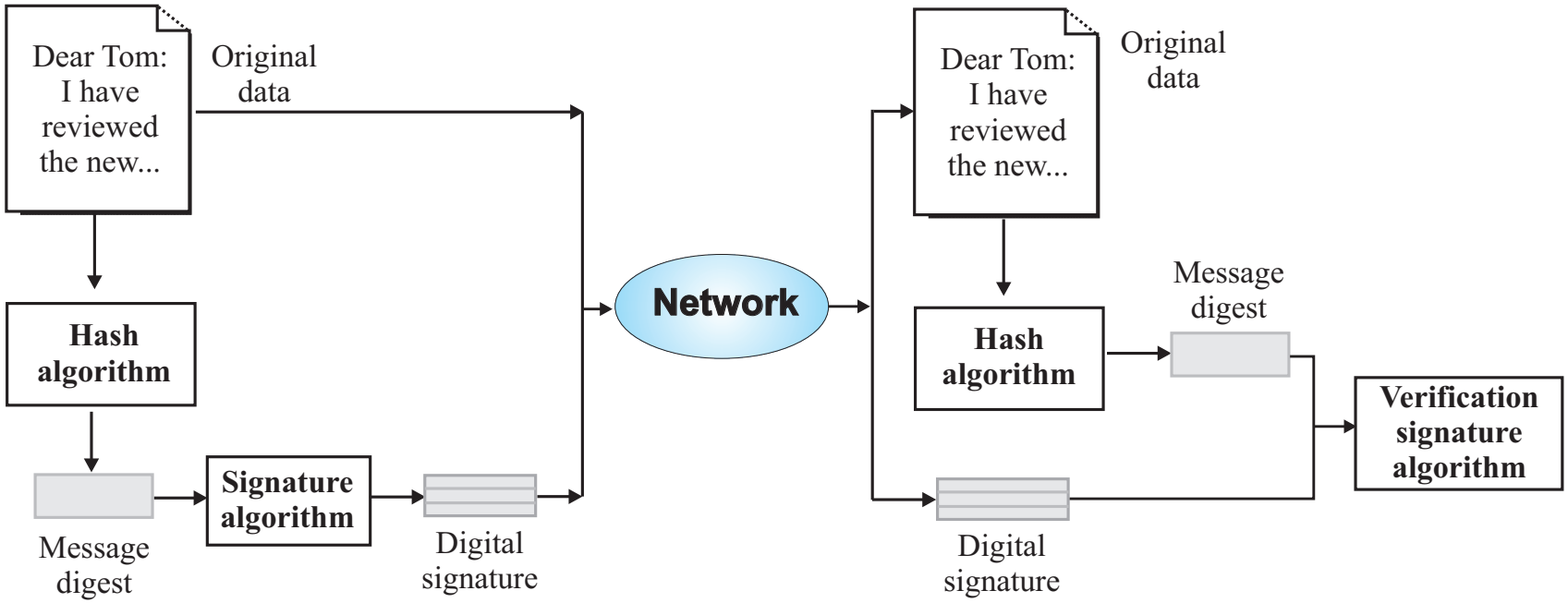
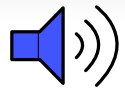


Figure: Hashing and digital signatures

Digital signatures from public key ciphers



Any public key cipher can 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:

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

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.

Outline

Threshold sharing schemes

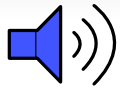
An important application of the Chinese remainder theorem concerns the construction of (k, n)-threshold sharing schemes.

Definition 5

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

- *$k \leq n$;*
- *each P_i has an information I_i;*
- *knowledge of any k of $I_1, \ldots, I_k$ enables one to find S easily;*
- *knowledge of less than k of $I_1, \ldots, I_k$ does not enable one to find S easily.*

Mignotte's threshold sharing schemes



We will show how a (k, n)-threshold sharing scheme can be constructed:

- let

$$\underbrace{m_1 < \cdots < m_k}_{\text{first } k \text{ numbers}} < \cdots < \underbrace{m_{n-k+2} < \cdots < m_n}_{\text{last } k-1 \text{ numbers}}$$

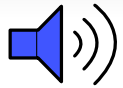
  be a sequence of pairwise co-prime numbers such that

$$\alpha = m_1 \cdots m_k > m_{n-k+2} \cdots m_n = \beta;$$

- let S be a secret, $\beta < S < \alpha$;
- each P_i gets the information $I_i = S \ mod \ m_i$.

This is called Mignotte's threshold sharing scheme.

Soundness of secret recovery



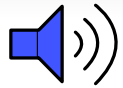
Any group of k people, $P_{i_1}, \ldots, P_{i_k}$, can recover uniquely the secret S by solving the system:

$$(*) \begin{cases} x & \equiv & I_{i_1} \ mod \ m_{i_1} \\ & \cdots & \\ x & \equiv & I_{i_k} \ mod \ m_{i_k} \end{cases}$$

According to the Chinese remainder theorem, this system has a unique solution modulo $m_{i_1} \cdots m_{i_k}$, and this solution is S because

$$S < \alpha \leq m_{i_1} \cdots m_{i_k}.$$

Security to coalition attack



No group of $k-1$ people, $P_{j_1}, \ldots, P_{j_k}$, can recover uniquely the secret S by solving the system:

$$(**) \begin{cases} x & \equiv & l_{j_1} \ mod \ m_{j_1} \\ & \cdots & \\ x & \equiv & l_{j_{k-1}} \ mod \ m_{j_{k-1}} \end{cases}$$

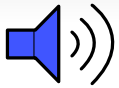
According to the Chinese remainder theorem, this system has a unique solution modulo $m_{j_1} \cdots m_{j_{k-1}}$, and this solution, denoted x_0, satisfies

$$x_0 < m_{j_1} \cdots m_{j_{k-1}} \leq \beta,$$

while $\beta < S$.

Outline

Course readings



1. F.L. Țiplea: *Fundamentele Algebrice ale Informaticii*, Ed. Polirom, Iași, 2006, pag. 268–283.

2. S. Iftene: *Secret Sharing Schemes with Applications in Security Protocols*, Ph.D. Thesis, "Al.I.Cuza" University of Iași, 2007, http://thor.info.uaic.ro/~tr/tr.pl.cgi.

3. C.C. Drăgan: *Security of CRT-based Secret Sharing Schemes*, Ph.D. Thesis, "Al.I.Cuza" University of Iași, 2013.