

Introduction and Asymmetric Encryption

Pascal Lafourcade

Université Joseph Fourier, Verimag

30 September 2009

Administrative Informations

Where & When

- ▶ 6 hours = 4 * 1h30 hours
- ▶ Mercredi 9h45

Instructor Information (I)

Address

- ▶ Instructor: Pascal Lafourcade
- ▶ Address:

VERIMAG, team DCS
Center Equation CTL
2, avenue de Vignate
38610 Gières

- ▶ Office: B4D CTL 1st floor
- ▶ Email: pascal.lafourcade@imag.fr
- ▶ Web: <http://www-verimag.imag.fr/~plafourc/>
- ▶ Phone: +33 (0) 4 56 52 04 21 (but email is better)
- ▶ Available most of the time in my office by appointment

Instructor Information (II)

Research in:

Information Security, Formal Verification (Symbolic, Computational), Cryptographic Protocols, Rewriting, Unification, Equational Theories, Constraints:

- ▶ e-voting
- ▶ e-auction
- ▶ Group protocols
- ▶ Wireless communications
- ▶ Tools
- ▶ Computational world
- ▶ ...

Web Pages

Courses Web Pages:

- ▶ Practical Informations online.
- ▶ Slides, homework, references, articles...

`www-verimag.imag.fr/~plafourc`

What about YOU?

Please fill the form.

Prerequisites

Some mathematical notions:

- ▶ a little number theory,
- ▶ ability to follow and do proofs,
e.g., proof by induction, contradiction...
- ▶ acquaintance with logic,
- ▶ ease with formal notation and manipulation,

but no advanced mathematics required.

Please see me if you have any doubt or question.

What is this course about?

A presentation to basics and essential notions, techniques, models used in security and cryptography.

Course topics, in details

- ▶ Introduction
- ▶ Asymmetric Encryption
- ▶ Symetric Encryption
- ▶ Security Notions
- ▶ Other Encryptions

Today: Introduction and Asymmetric Encryption

Contents (I)

Security touches many domains:

- ▶ cryptography,
- ▶ mathematics,
- ▶ operating system,
- ▶ networking,

We should at least touch most of these topics, but we will not try to cover all aspects of security.

Contents (II)

- ▶ Not a complete course on cryptography,
- ▶ Not a complete course on security.

Reading

Required reading:

- ▶ No textbook!
- ▶ Many papers, indicated during the course.

Some recommended book:

- ▶ Bruce Schneier “Applied cryptography” ,
- ▶ Matt Bishop “Computer Security: Art and Science” ,
- ▶ Douglas Stinson “Cryptography: Theory and Practice” ,
- ▶ Two volumes of:
“The Foundations of Cryptography” by Oded Goldreich
- ▶ For background on cryptography, online book:
“The handbook of applied cryptography” by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone.
www.cacr.math.uwaterloo.ca/hac/index.html
- ▶ Simon Singh “The Code Book: The Secret History of Codes and Code Breaking” .
- ▶ More online during the semester

Course work

- ▶ Reading.
- ▶ Class participation.
- ▶ Homework:
 - ▶ Given and explained in class,
 - ▶ Given in the slides,
 - ▶ Usually due at the start of class one week later.

Outline

Presentation

Motivations

History of Cryptography

Classical Asymmetric Encryptions

Conclusion

Outline

Presentation

Motivations

History of Cryptography

Classical Asymmetric Encryptions

Conclusion

Typical security-critical problems

- ▶ **Secure communication**, e.g., via telephone, email, fax.
Objective: confidentiality and integrity of transmitted information.
- ▶ **Internet banking.** **Objectives:** confidentiality of transactions and account information, prevention of false transactions, impossibility of repudiating (denying) a transaction by a user,
...
- ▶ **Digital payment systems.**
- ▶ **E-voting systems, ...**

N.B.: specifying objectives (security properties) is not always easy.
Neither is building systems that satisfy these objectives!

Traditional security properties

- ▶ Common security properties are:
 - **Confidentiality or Secrecy**: No improper disclosure of information
 - **Authentication**: To be sure to talk with the right person.
disclosure of information
 - **Integrity**: No improper modification of information
 - **Availability**: No improper impairment of functionality/service

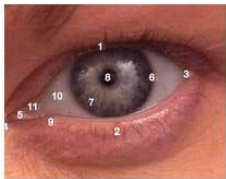
Authentication



"On the Internet, nobody knows you're a dog."

Mechanisms for Authentication

1. Something that you know
E.g. a PIN or a password
2. Something that you have
E.g. a smart-card
3. Something that you are
Biometric characteristics like voice, fingerprints, eyes, ...
4. Where you are located
E.g. in a secure building



Strong authentication combines multiple factors:
E.g., Smart-Card + PIN

Other security properties

- ▶ **Non-repudiation** (also called **accountability**) is where one can establish responsibility for actions.
- ▶ **Fairness** is the fact there is no advantage to play one role in a protocol comparing with the other ones.
- ▶ **Privacy**
 - Anonymity**: secrecy of principal identities or communication relationships.
 - Pseudonymity**: anonymity plus link-ability.
 - Data protection**: personal data is only used in certain ways.

Example: banking

- ▶ A bank may require
 - ▶ authenticity of clients (at teller, ATMs, or on the Internet),
 - ▶ non-repudiation of transactions,
 - ▶ integrity of accounts and other customer data,
 - ▶ secrecy of customer data, and
 - ▶ availability of logging.
- ▶ The conjunction of these properties might constitute the bank's (high-level) security policy.

Another example: e-voting

- ▶ An e-voting system should ensure that
 - ▶ only registered voters vote,
 - ▶ each voter can only vote once,
 - ▶ integrity of votes,
 - ▶ privacy of voting information (only used for tallying), and
 - ▶ availability of system during voting period
- ▶ In practice, many policy aspects are difficult to formulate precisely.

Exercise (Due to next course): Give the security properties that an international airport should guarantee.

Outline

Presentation

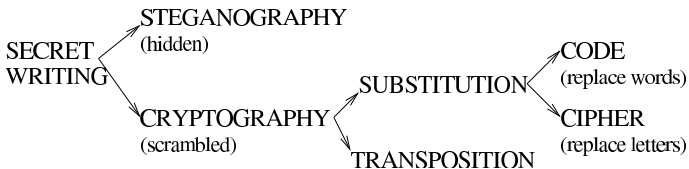
Motivations

History of Cryptography

Classical Asymmetric Encryptions

Conclusion

Information hiding



- ▶ **Cryptology**: the study of secret writing.
- ▶ **Steganography**: the science of hiding messages in other messages.
- ▶ **Cryptography**: the science of secret writing.
Note: terms like **encrypt**, **encode**, and **encipher** are often (loosely and wrongly) used interchangeably

Slave



Kerchoffs Principle

In 1883, a Dutch linguist Auguste Kerchoff von Nieuwenhof stated in his book “La Cryptographie Militaire” that:

“the security of a crypto-system must be totally dependent on the secrecy of the key, not the secrecy of the algorithm.”

Authors name sometimes spelled Kerckhoff

Symmetric key and public key encryption

- Symmetric key encryption



- Public key encryption



Historical ciphers

- ▶ Used 4000 years ago by Egyptians to encipher hieroglyphics.



- ▶ Ancient Hebrews enciphered certain words in the scriptures.
- ▶ 2000 years ago Julius Caesar used a simple substitution cipher.
- ▶ Roger Bacon described several methods in 1200s.
- ▶ Geoffrey Chaucer included several ciphers in his works.
- ▶ Leon Alberti devised a cipher wheel, and described the principles of frequency analysis in the 1460s.

Mono-alphabetic substitution ciphers

- ▶ Simplest kind of cipher. Idea over 2,000 years old.
- ▶ Let \mathcal{K} be the set of all permutations on the alphabet \mathcal{A} . Define for each $e \in \mathcal{K}$ an encryption transformation E_e on strings $m = m_1 m_2 \cdots m_n \in \mathcal{M}$ as

$$E_e(m) = e(m_1)e(m_2) \cdots e(m_n) = c_1 c_2 \cdots c_n = c.$$

- ▶ To decrypt c , compute the inverse permutation $d = e^{-1}$ and

$$D_d(c) = d(c_1)d(c_2) \cdots d(c_n) = m.$$

- ▶ E_e is a **simple substitution cipher** or a **mono-alphabetic substitution cipher**.

Substitution cipher examples

- ▶ KHOOR ZRUOG

Substitution cipher examples

- ▶ KHOOR ZRUOG = HELLO WORLD

Caesar cipher: each plaintext character is replaced by the character three to the right modulo 26.

Substitution cipher examples

- ▶ KHOOR ZRUOG = HELLO WORLD
Caesar cipher: each plaintext character is replaced by the character three to the right modulo 26.
- ▶ Zl anzr vf Nqnz

Substitution cipher examples

- ▶ KHOOR ZRUOG = HELLO WORLD
Caesar cipher: each plaintext character is replaced by the character three to the right modulo 26.
- ▶ Zl anzr vf Nqnz = My name is Adam
ROT13: shift each letter by 13 places.
Under Unix: `tr a-zA-Z n-za-mN-ZA-M`.
- ▶ 2-25-5 2-25-5

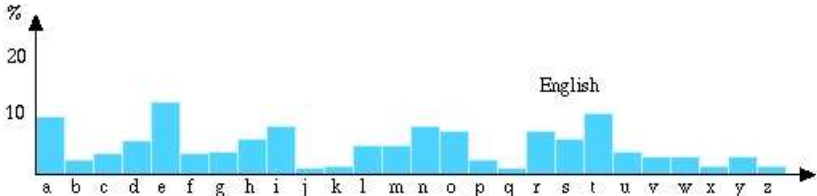
Substitution cipher examples

- ▶ KHOOR ZRUOG = HELLO WORLD
Caesar cipher: each plaintext character is replaced by the character three to the right modulo 26.
- ▶ Zl anzr vf Nqnz = My name is Adam
ROT13: shift each letter by 13 places.
Under Unix: `tr a-zA-Z n-za-mN-ZA-M.`
- ▶ 2-25-5 2-25-5 = BYE BYE
Alphanumeric: substitute numbers for letters.

How hard are these to cryptanalyze? Caesar? General?

(In)security of substitution ciphers

- ▶ Key spaces are typically huge. 26 letters \rightsquigarrow 26! possible keys.
- ▶ Trivial to crack using frequency analysis (letters, digraphs...)
- ▶ Frequencies for English based on data-mining books/articles.



How to break a monoalphabetic cipher

- ▶ Guess the target language
- ▶ Count letter frequencies in the cryptogram C
- ▶ Match cryptogram's frequencies with language's frequencies
- ▶ Use the partially decrypted message to correct errors.

Example

WYSKBO KT CZWJB RCBTKAJSJA WC HJ WIJ ZGWIJS CZ MCAJSB RCMDYWJS TRKJBRJ. WYSKBO
 DSCFKAJA GB KBZLYJBWKGL ZCSMGLKTGWKCB CZ WIJ RCBRJW CZ WIJ GLOCSKWM GBA RCMDYWGKCB NKWI WIJ
 WYSKBO MGRIKBJ. NKWI WIJ WYSKBO WJTW, IJ MGAJ G TKOBKZKRGBW GBA RIGSGRWJSKTWKRGLLX DSCFCRGWKFJ
 RCBWSKHYWKCB WC WIJ AJHGJW SJOGSAKBO GSWKZKRKGL KBWJLLKOJBRJ: NIJWIJS KW NKLL JFJS HJ DCTTKHLJ
 WC TGX WIGW G MGRIKBJ KT RCBTRKCYT GBA RGB WIKBV. IJ LGWJS NCSVJA GW WIJ BGWKCBL DIXTKRGL
 LGHCSGWCSX, RSJGWKBO CBJ CZ WIJ ZKSTW AJTKOBT ZCS G TWCSJA-DSCOSGM RCMDYWJS, GLWICYOI KW NGT

BJFJS GRWYGLLX HYKLW. Frequencies: W (54), J (49), K (45), G (41), C (35),
 B (35), S (32), I (24), R (24), L (20), T (19), A (14), O (13), Y (13), Z
 (12), M (10), D (9), H (7), N (6), F (5), X (5), V (2). Frequencies in
 english: "ETAOIN SHRDLU".

Example Try $T \rightarrow W$ and $E \rightarrow J$:

TYSKBO KW CZTEB RCBWKAESEA TC HE TIE ZGTIES CZ MCAESB RCMDYTES WRKEBRE. TYSKBO DSCFKAEA GB
 KBZLYEBTKGL ZCSMGLKWGTKCB CZ TIE RCBREDT CZ TIE GLOCKTIM GBA RCMDYTGTKCB NKTIE TIE TYSKBO
 MGRIKBE. NKTIE TIE TYSKBO TEWT, IE MGAE G WKOBKZKRGBT GBA RIGSGRTEKWKTRGLLX DSCFCRGTKFE
 RCBTSKHYTKCB TC TIE AEHGTE SEOGSAKBO GSTKZKRKGL KBTELLKOE BRE: NIETIES KT NKLL EFES HE DCWVKHLE
 TC WGX TIGT G MGRIKBE KW RCBWRKCYW GBA RGB TIKBV. IE LGTES NCSVEA GT TIE BGTKCBGL DIXWKRL
 LGHCSGTCSX, RSEGTKBO CBE CZ TIE ZKSWT AEWKOBW ZCS G WTCSEA-DSCOSGM RCMDYTES, GLTICYOI KT NGW
 BEFES GRTYGLLX HYKLT. Frequencies: W (54), J (49), K (45), G (41), C (35),
 B (35), S (32), I (24), R (24), L (20), T (19), A (14), O (13), Y (13), Z
 (12), M (10), D (9), H (7), N (6), F (5), X (5), V (2).

Example Guess that TIE is THE and assume $H \rightarrow I$:

TYSKBO KW CZTEB RCBWKAEESEA TC IE THE ZGTHES CZ MCAESB RCMDYTES WRKEBRE. TYSKBO DSCFKAEA GB
 KBZLYEBTKGL ZCSMGLKWGTKCB CZ THE RCBREDT CZ THE GLOCSKTHM GBA RCMDYTGTKCB NKTH THE TYSKBO
 MGRHKBE. NKTH THE TYSKBO TEWT, HE MGAE G WKOBKZKRGBT GBA RHGSGRTESKWTKRGLLX DSCFCRGTKFE
 RCBTSKIYTKCB TC THE AEIGTE SEOGSAKBO GSTKZKRKGL KBTLLKOE BRE: NHETHES KT NKLL EFES IE DCWWKILE
 TC WGX THGT G MGRHKBE KW RCBWRKCYW GBA RGB THKBV. HE LGTES NCSVEA GT THE BGTKCBGL DHXWKRL
 LGICSGTCSX, RSEGTKBO CBE CZ THE ZKSWT AEWKOBW ZCS G WTCSEA-DSCOSGM RCMDYTES, GLTHCYOH KT NGW
 BEFES GRTYGLLX IYKLT.

Frequencies: W (54), J (49), K (45), G (41), C (35), B (35), S (32), I
 (24), R (24), L (20), T (19), A (14), O (13), Y (13), Z (12), M (10), D
 (9), H (7), N (6), F (5), X (5), V (2).

Example Single letter-word 'G': guess that A \rightarrow G:

TYSKBO KW CZTEB RCBWKGESEG TC IE THE ZATHES CZ MCGESB RCMDYTES WRKEBRE. TYSKBO DSCFKGEG AB
 KBZLYEBTKAL ZCSMALKWATKCB CZ THE RCBREDT CZ THE ALOCSKTHM ABG RCMDYTATKCB NKTH THE TYSKBO
 MARHKBE. NKTH THE TYSKBO TEWT, HE MAGE A WKOBKZKRABT ABG RHASARTESKWTKRALLX DSCFCRATKFE
 RCBTSKIYTKCB TC THE GEIATE SEOASGKBO ASTKZKRKAL KBTELLKOE BRE: NHETHES KT NKLL EFES IE DCWWKILE
 TC WAX THAT A MARHKBE KW RCBWRKCYW ABG RAB THKBV. HE LATES NCSVEG AT THE BATKCBAL DHXWKRAL
 LAICSATCSX, RSEATKBO CBE CZ THE ZKSWT GEWKOBW ZCS A WTCSEG-DSCOSAM RCMDYTES, ALTHCYOH KT NAW
 BEFES ARTYALLX IYKLT. Frequencies: W (54), J (49), K (45), G (41), C (35),
 B (35), S (32), I (24), R (24), L (20), T (19), A (14), O (13), Y (13), Z
 (12), M (10), D (9), H (7), N (6), F (5), X (5), V (2).

Example Further guess consistent with frequencies: $O \rightarrow C$, $I \rightarrow K$,
 $N \rightarrow B$.

TYSINC IW OZTEN RONWIGESEG TO HE THE ZATHES OZ MOGESN ROMDYTES WRIENRE. TYSINC DSOFIGEG AN
 INZLYENTIAL ZOSMALIWATION OZ THE RONREDT OZ THE ALCOSITHM ANG ROMDYTATION BITH THE TYSINC
 MARHINE. BITH THE TYSINC TEWT, HE MAGE A WICNIZIRANT ANG RHASARTESIWTIRALLX DSOFORATIFE
 RONTSIHYTION TO THE GEHATE SECASGINC ASTIZIRIAL INTELLICENRE: BHETHES IT BILL EFES HE DOWWIHLE
 TO WAX THAT A MARHINE IW RONWRIOYW ANG RAN THINV. HE LATES BOSVEG AT THE NATIONAL DHXWIRAL
 LAHOSATOSX, RSEATING ONE OZ THE ZISWT GEWICNW ZOS A WTOSEG-DSOCSAM ROMDYTES, ALTHOYCH IT BAW
 NEFES ARTYALLX HYILT. Frequencies: W (54), J (49), K (45), G (41), C (35),
 B (35), S (32), I (24), R (24), L (20), T (19), A (14), O (13), Y (13), Z
 (12), M (10), D (9), H (7), N (6), F (5), X (5), V (2).

Example We're almost done! Guess that ALCOSITHM is ALGORITHM, MARHINE is MACHINE. Clear text:

TURING IS OFTEN CONSIDERED TO BE THE FATHER OF MODERN COMPUTER SCIENCE. TURING PROVIDED AN INFLUENTIAL FORMALISATION OF THE CONCEPT OF THE ALGORITHM AND COMPUTATION WITH THE TURING MACHINE. WITH THE TURING TEST, HE MADE A SIGNIFICANT AND CHARACTERISTICALLY PROVOCATIVE CONTRIBUTION TO THE DEBATE REGARDING ARTIFICIAL INTELLIGENCE: WHETHER IT WILL EVER BE POSSIBLE TO SAY THAT A MACHINE IS CONSCIOUS AND CAN THINK. HE LATER WORKED AT THE NATIONAL PHYSICAL LABORATORY, CREATING ONE OF THE FIRST DESIGNS FOR A STORED-PROGRAM COMPUTER, ALTHOUGH IT WAS NEVER ACTUALLY BUILT.

Example We're almost done! Guess that ALCOSITHM is ALGORITHM, MARHINE is MACHINE. Clear text:

TURING IS OFTEN CONSIDERED TO BE THE FATHER OF MODERN COMPUTER SCIENCE. TURING PROVIDED AN INFLUENTIAL FORMALISATION OF THE CONCEPT OF THE ALGORITHM AND COMPUTATION WITH THE TURING MACHINE. WITH THE TURING TEST, HE MADE A SIGNIFICANT AND CHARACTERISTICALLY PROVOCATIVE CONTRIBUTION TO THE DEBATE REGARDING ARTIFICIAL INTELLIGENCE: WHETHER IT WILL EVER BE POSSIBLE TO SAY THAT A MACHINE IS CONSCIOUS AND CAN THINK. HE LATER WORKED AT THE NATIONAL PHYSICAL LABORATORY, CREATING ONE OF THE FIRST DESIGNS FOR A STORED-PROGRAM COMPUTER, ALTHOUGH IT WAS NEVER ACTUALLY BUILT.

- ▶ Easy to apply, except for short, atypical texts

From Zanzibar to Zambia and Zaire, ozone zones make zebras run zany zigzags.

⇒ More sophistication required to mask statistical regularities.

Homophonic substitution ciphers

- ▶ To each $a \in \mathcal{A}$, associate a set $H(a)$ of strings of t symbols, where $H(a), a \in \mathcal{A}$ are pairwise disjoint. A **homophonic substitution cipher** replaces each a with a randomly chosen string from $H(a)$. To decrypt a string c of t symbols, one must determine an $a \in \mathcal{A}$ such that $c \in H(a)$. The key for the cipher is the sets $H(a)$.
- ▶ **Example:** $\mathcal{A} = \{a, b\}$, $H(a) = \{00, 10\}$, and $H(b) = \{01, 11\}$. The plaintext ab encrypts to one of 0001, 0011, 1001, 1011.
- ▶ Rational: makes frequency analysis more difficult.
Cost: data expansion and more work for decryption.

Polyalphabetic substitution ciphers

- ▶ Idea (Leon Alberti): conceal distribution using family of mappings.



- ▶ A **polyalphabetic substitution cipher** is a block cipher with block length t over alphabet \mathcal{A} where:
 - ▶ the key space \mathcal{K} consists of all ordered sets of t permutations over \mathcal{A} , (p_1, p_2, \dots, p_t) .
 - ▶ Encryption of $m = m_1 \cdots m_t$ under key $e = (p_1, \dots, p_t)$ is $E_e(m) = p_1(m_1) \cdots p_t(m_t)$.
 - ▶ Decryption key for e is $d = (p_1^{-1}, \dots, p_t^{-1})$.

Example: Vigenère ciphers

- ▶ Key given by sequence of numbers $e = e_1, \dots, e_t$, where

$$p_i(a) = (a + e_i) \bmod n$$

defining a permutation on an alphabet of size n .

- ▶ Example: English ($n = 26$), with $k = 3,7,10$

$m =$ THI SCI PHE RIS CER TAI NLY NOT SEC URE

then

$E_e(m) =$ WOS VJS SOO UPC FLB WHS QSI QVD VLM XYO

One-time pads (Vernam cipher)

- ▶ A **one-time pad** is a cipher defined over $\{0, 1\}$. Message $m_1 \cdots m_n$ is encrypted by a binary key string $k_1 \cdots k_n$.

$$E_{k_1 \cdots k_n}(m_1 \cdots m_n) = (m_1 \oplus k_1) \cdots (m_n \oplus k_n)$$

$$D_{k_1 \cdots k_n}(c_1 \cdots c_n) = (c_1 \oplus k_1) \cdots (c_n \oplus k_n)$$

- ▶ Example:
$$\begin{array}{r} m = 010111 \\ k = 110010 \\ \hline c = 100101 \end{array}$$

- ▶ Since every key sequence is equally likely, so is every plaintext! Unconditional (information theoretic) security, if key isn't reused!
- ▶ Moscow–Washington communication previously secured this way.
- ▶ Problem?

One-time pads (Vernam cipher)

- ▶ A **one-time pad** is a cipher defined over $\{0, 1\}$. Message $m_1 \cdots m_n$ is encrypted by a binary key string $k_1 \cdots k_n$.

$$E_{k_1 \cdots k_n}(m_1 \cdots m_n) = (m_1 \oplus k_1) \cdots (m_n \oplus k_n)$$

$$D_{k_1 \cdots k_n}(c_1 \cdots c_n) = (c_1 \oplus k_1) \cdots (c_n \oplus k_n)$$

- ▶ Example:
$$\begin{array}{r} m = 010111 \\ k = 110010 \\ \hline c = 100101 \end{array}$$

- ▶ Since every key sequence is equally likely, so is every plaintext! Unconditional (information theoretic) security, if key isn't reused!
- ▶ Moscow–Washington communication previously secured this way.
- ▶ Problem? Securely exchanging and synchronizing long keys.

Transposition ciphers

- ▶ For block length t , let \mathcal{K} be the set of permutations on $\{1, \dots, t\}$. For each $e \in \mathcal{K}$ and $m \in \mathcal{M}$

$$E_e(m) = m_{e(1)}m_{e(2)} \cdots m_{e(t)}.$$

- ▶ The set of all such transformations is called a **transposition cipher**.
- ▶ To decrypt $c = c_1 c_2 \cdots c_t$ compute $D_d(c) = c_{d(1)}c_{d(2)} \cdots c_{d(t)}$, where d is inverse permutation.
- ▶ Letters unchanged so frequency analysis can be used to reveal if ciphertext is a transposition. Decrypt by exploiting frequency analysis for diphthongs, triphthongs, words, etc.

Example: transposition ciphers

▶ $C = \text{Aduaenttlydhatoiekounletmtoiha hvsekeeeleeyqonouv}$

Example: transposition ciphers

- $C = \text{Aduaenttlydhatoiekounletmtoiha hvsekeeeleeyqonouv}$

A	n	d	i	n	t	h	e	e	n
d	t	h	e	l	o	v	e	y	o
u	t	a	k	e	i	s	e	q	u
a	l	t	o	t	h	e	l	o	v
e	y	o	u	m	a	k	e		

Table defines a permutation on $1, \dots, 50$.

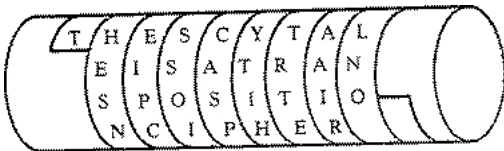
Example: transposition ciphers

- ▶ $C = \text{Aduaenttlydhatoiekounletmtoiha hvsekeeeleyqonouv}$

A	n	d	i	n	t	h	e	e	n
d	t	h	e	l	o	v	e	y	o
u	t	a	k	e	i	s	e	q	u
a	l	t	o	t	h	e	l	o	v
e	y	o	u	m	a	k	e		

Table defines a permutation on $1, \dots, 50$.

- ▶ Idea goes back to Greek **Scytale**: wrap belt spirally around baton and write plaintext lengthwise on it.



Composite ciphers

- ▶ Ciphers based on just substitutions or transpositions are not secure
- ▶ Ciphers can be combined. However . . .
 - ▶ two substitutions are really only one more complex substitution,
 - ▶ two transpositions are really only one transposition,
 - ▶ but a substitution followed by a transposition makes a new harder cipher.
- ▶ Product ciphers chain substitution-transposition combinations.
- ▶ Difficult to do by hand
↪ invention of cipher machines.



ENIGMA

Three-rotor German military Enigma machine

Dayly keys are used and stored in a book.

There are 10^{14} possibilities for one cipher.



Other German Tricks

A space was omitted or replaced by an X. The X was generally used as point or full stop. They replaced the comma by Y and the question sign by UD. The combination CH, as in "Acht" (eight) or "Richtung" (direction) were replaced by Q (AQT, RIQTUNG).



Shannon's Principle 1949

Confusion

The purpose of confusion is to make the relation between the key and the ciphertext as complex as possible.

Ciphers that do not offer much confusion (such as Vigenere cipher) are susceptible to frequency analysis.

Shannon's Principle 1949

Confusion

The purpose of confusion is to make the relation between the key and the ciphertext as complex as possible.

Ciphers that do not offer much confusion (such as Vigenere cipher) are susceptible to frequency analysis.

Diffusion

Diffusion spreads the influence of a single plaintext bit over many ciphertext bits.

The best diffusing component is substitution (homophonic)

Shannon's Principle 1949

Confusion

The purpose of confusion is to make the relation between the key and the ciphertext as complex as possible.

Ciphers that do not offer much confusion (such as Vigenere cipher) are susceptible to frequency analysis.

Diffusion

Diffusion spreads the influence of a single plaintext bit over many ciphertext bits.

The best diffusing component is substitution (homophonic)

Principle

A good cipher design uses Confusion and Diffusion together

Outline

Presentation

Motivations

History of Cryptography

Classical Asymmetric Encryptions

Conclusion

One-way function and Trapdoor

Definition

A function is *One-way*, if :

- ▶ it is easy to compute
- ▶ its inverse is hard to compute :

$$\Pr[m \xleftarrow{r} \{0, 1\}^*; y := f(m) : f(\mathcal{A}(y, f)) = m]$$

is negligible.

Trapdoor:

- ▶ Inverse is easy to compute given an additional information (an inverse key e.g. in RSA).

Integer Factoring

→ Use of algorithmically hard problems.

Factorization

- ▶ $p, q \mapsto n = p \cdot q$ easy (quadratic)
- ▶ $n = p \cdot q \mapsto p, q$ difficult

RSA

RSA function $n = pq$, p and q primes.

e : public exponent

- ▶ $x \mapsto x^e \pmod n$ easy (cubic)
- ▶ $y = x^e \mapsto x \pmod n$ difficult
 $x = y^d$ where $d = e^{-1} \pmod{\phi(n)}$

Soundness

Assume $n = pq$, $\gcd(e, \phi(n)) = 1$ and $d = e^{-1} \pmod{\phi(n)}$.

$$c^d = m^{de} = m \cdot m^{k\phi(n)} \pmod n$$

According to the Fermat Little Theorem $\forall x \in (\mathbb{Z}/n\mathbb{Z})^*$, $x^{\phi(n)} = 1$

Example RSA

Example

- ▶ $p = 61$ (destroy this after computing E and D)
- ▶ $q = 53$ (destroy this after computing E and D)
- ▶ $n = pq = 3233$ modulus (give this to others)
- ▶ $e = 17$ public exponent (give this to others)
- ▶ $d = 2753$ private exponent (keep this secret!)

Your public key is (e, n) and your private key is d .

$$\text{encrypt}(T) = (T^e) \bmod n = (T^{17}) \bmod 3233$$

$$\text{decrypt}(C) = (C^d) \bmod n = (C^{2753}) \bmod 3233$$

- ▶ $\text{encrypt}(123) = 123^{17} \bmod 3233$
 $= 337587917446653715596592958817679803 \bmod 3233$
 $= 855$
- ▶ $\text{decrypt}(855) = 855^{2753} \bmod 3233$

Complexity Estimates

Estimates for integer factoring Lenstra-Verheul 2000

Modulus (bits)	Operations (\log_2)
512	58
1024	80
2048	111
4096	149
8192	156

$\approx 2^{60}$ years

→ Can be used for RSA too.

ElGamal Encryption Scheme

Key generation: Alice chooses a prime number p and a group generator g of $(\mathbb{Z}/p\mathbb{Z})^*$ and $a \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$.

Public key: (p, g, h) , where $h = g^a \pmod p$.

Private key: a

Encryption: Bob chooses $r \in_R (\mathbb{Z}/(p-1)\mathbb{Z})^*$ and computes

$$(u, v) = (g^r, Mh^r)$$

Decryption: Given (u, v) , Alice computes $M \equiv_p \frac{v}{u^a}$

Justification: $\frac{v}{u^a} = \frac{Mh^r}{g^{ra}} \equiv_p M$

Remarque: re-usage of the same random r leads to a security flaw:

$$\frac{M_1 h^r}{M_2 h^r} \equiv_p \frac{M_1}{M_2}$$

Practical Inconvenience: Cipher is twice as long as plain text.

Outline

Presentation

Motivations

History of Cryptography

Classical Asymmetric Encryptions

Conclusion

Summary

Today

- ▶ Presentation
- ▶ Motivation
- ▶ History of Cryptography
- ▶ Classical Asymmetric Encryption

Next Time

- ▶ Classical Symmetric Encryption
- ▶ Security Notions
- ▶ Others encryptions

Thank you for your attention

Questions ?