

Introduction

Pascal Lafourcade

Université Joseph Fourier, Verimag

September 13th 2010

Equipe enseignante

- ▶ Philippe Elbaz-Vincent
- ▶ Laurent Fousse
- ▶ Pascal Lafourcade

Détails des cours

1. Lundi 13 septembre **Historique de la cryptographie** (PL)
2. Lundi 20 septembre **Chiffrements Symétriques** (LF)
3. Lundi 27 septembre **Protocoles** (PL)
4. Lundi 4 octobre **Fonctions de Hachage** (LF)
5. Lundi 11 octobre
Chiffrements asymétriques et applications (PEV)
6. Lundi 18 octobre **Trouver des failles avec un ordinateur B110** (PL)
7. Lundi 8 novembre
Cryptanalyse des chiffrements asymétriques I (PEV)
8. Lundi 15 novembre
Cryptanalyse des chiffrements asymétriques II (PEV)
9. Lundi 22 novembre **Applications : E-voting, ...** (PL)
10. Lundi 29 novembre **Ouverture: courbes elliptiques ...** (LF)

Today: Historique de la cryptographie.

Administrative Informations

Where & When

- ▶ 20 hours = 10 * 2h00 hours
- ▶ Room E202 DLST
- ▶ TP 18th October room B110
- ▶ Monday 17h00 - 19h00

Instructor Information (I)

Address

- ▶ Instructor: Pascal Lafourcade
- ▶ Address:

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

- ▶ Office: B1D 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/teaching/L2_Magistere_2010_2011.php

What about YOU?

Please fill the form.

Prerequisites

NONE

- ▶ Just like Mathematics
- ▶ a little number theory can help sometime.

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.

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
- ▶ Jonathan Katz and Yehuda Lindell “Introduction to modern cryptography”
- ▶ Simon Singh “The Code Book: The Secret History of Codes and Code Breaking”.
- ▶ More online during the semester

Grades are based on the project

- ▶ One subject for two persons by project.
- ▶ Team and subjects due to 18th October.
- ▶ Report due to first week of January 2009
- ▶ Presentation middle of January 2009

Magister L2 S1 = 50 % Presentation + 50 % Report.

First Draft of the Project's List

- ▶ Elgamal, RSA
- ▶ DES (changer Sbox, cryptanalyse)
- ▶ AES (changer les Boxes, DPA) (Minier)
- ▶ MD5, SHA1, IDEA
- ▶ Water marking
- ▶ Courbes Eliptiques (algorithms ...)
- ▶ Cryptanalyse
- ▶ Merkle-Hellman
- ▶ E-voting protocols
- ▶ E-auction Protocols
- ▶ Implantation ZKP, Secret Sharing
- ▶ Weakness of RC4
- ▶ Survey et performance Chiffrement Symmetrique
- ▶ Biometrics

Open subject, open mind ...

Outline

Presentation

Outline

Presentation

Motivations

Outline

Presentation

Motivations

History of Cryptography

Outline

Presentation

Motivations

History of Cryptography

Exercises

Outline

Presentation

Motivations

History of Cryptography

Exercises

Challenge

Outline

Presentation

Motivations

History of Cryptography

Exercises

Challenge

Conclusion

Outline

Presentation

Motivations

History of Cryptography

Exercises

Challenge

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.
- ▶ Digital rights management.

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

Traditional security properties

- ▶ Policies are often formulated to achieve certain standard security properties (also called security goals)
- ▶ Common security properties are:
 - Confidentiality or Secrecy: No improper disclosure of information
 - Integrity: No improper modification of information
 - Availability: No improper impairment of functionality/service
- ▶ Note that: (Im)proper must be specified individually, for each system.

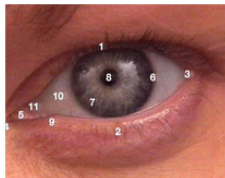
Authentication



"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.
- ▶ **Plausible deniability** is contrary to non-repudiation and can be seen as weak form of secrecy.
- ▶ **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 (NOW): Give the security properties that an international airport should guarantee.

Outline

Presentation

Motivations

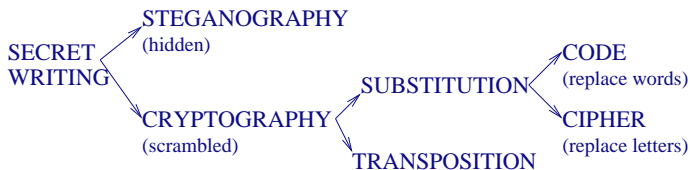
History of Cryptography

Exercises

Challenge

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

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 $m = m_1m_2 \cdots m_n \in \mathcal{M}$ as

$$E_e(m) = e(m_1)e(m_2) \cdots e(m_n) = c_1c_2 \cdots c_n = c.$$

- ▶ 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**.

Security ?

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 $m = m_1m_2 \cdots m_n \in \mathcal{M}$ as

$$E_e(m) = e(m_1)e(m_2) \cdots e(m_n) = c_1c_2 \cdots c_n = c.$$

- ▶ 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**.

Security ? very weak, try the 26 possibilities ;-)

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 anrz 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

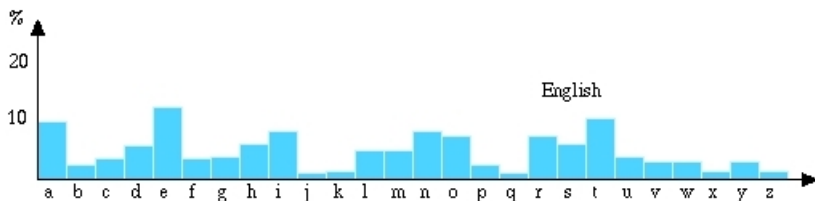
Substitution cipher examples

- ▶ KHOOR ZRUOG = HELLO WORLD
Caesar cipher: each plaintext character is replaced by the character three to the right modulo 26.
- ▶ Zl anrz 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 RCBRJDW CZ WIJ GLOCSKIM GBA RCMDYWGWKCB NKWI WIJ WYSKBO
 MGRIKBJ. NKWI WIJ WYSKBO WJTW, IJ MGAJ G TKOBKZKRGBW GBA RIGSGRWJSKTWKRGLLX DSCFCRGWKFJ
 RCBWSKHYWKCB WC WIJ AJHGWI SJOGSAKBO GSWKZKRKGL KBWJLLKOJBRJ: NIJWIJS KW NKLL JFJS HJ DCTTKHLJ
 WC TGX WIGW G MGRIKBJ KT RCBTRKCYT GBA RGB WIKBV. IJ LGWJS NCSVJA GW WIJ BGWKCGL 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 RCBWKAESSEA TC HE TIE ZGTIES CZ MCAESB RCMDYTES WRKEBRE. TYSKBO DSCFKAEA GB
 KBZLYEBTKGL ZCSMGLKWGTKCB CZ TIE RCBREDT CZ TIE GLOCSKTIM GBA RCMDYTGTKCB NKTIE TIE TYSKBO
 MGRIKBE. NKTIE TIE TYSKBO TEWT, IE MGAE G WKOBKZKRGBT GBA RIGSGRTEKWKTRGLLX DSCFCRGTKFE
 RCBTSKHYTKCB TC TIE AEHGTE SEOGSAKBO GSTKZKRKGL KBTELLKOEBS: NIETIES KT NKLL EFES HE DCWWKHLE
 TC WGX TIGT G MGRIKBE KW RCBWRKCYW GBA RGB TIKBV. IE LGTES NCSVEA GT TIE BGTKCBGL DIXWKRGL
 LGHCSGTC SX, 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 RCBWKAEMEA TC IE THE ZGTHES CZ MCAESB RCMYTES 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 RHGSGRTEKSWTKRGLLX DSCFCRGTKFE RCBTSKIYTKCB TC THE AEIGTE SEOGSAKBO GSTKZKRKGL KBTLLKOEKRE: NHETHES KT NKLL EFES IE DCWWKILE TC WGX THGT G MGRHKBE KW RCBWRKCYW GBA RGB THKBV. HE LGTES NCSVEA GT THE BGTKCBGL DHXWKRGL LGICSGTCSX, RSEGTKBO CBE CZ THE ZKSWT AEWKOBW ZCS G WTCSEA-DSCOSGM RCMYTES, 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 RCBWKGEGEG 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 RONWIGESG TO HE THE ZATHES OZ MOGESN ROMDYTES WRLENRE. 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, RSEATINC 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 $k_1 \cdots k_n$.

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

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

$$m = 010111$$

- ▶ Example: $k = 110010$
-
- $$c = 100101$$

- ▶ 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.

A more precise proof of security: Entropy

Entropy

For a random variable X which takes a finite number of values x define

$$H(X) = - \sum_x \Pr[X = x] \log_2(\Pr[X = x])$$

A more precise proof of security: Entropy

Joint entropy

For two random variables X, Y which takes a finite number of values x, y define

$$H(X, Y) = - \sum_{x,y} \Pr[X = x, Y = y] \log_2(\Pr[X = x, Y = y])$$

A more precise proof of security: Entropy

Conditional entropy

For two random variables X, Y which takes a finite number of values and y a possible value of Y define

$$H(X|y) = - \sum_x \Pr[X = x|Y = y] \log_2(\Pr[X = x|Y = y])$$

and summing with ponderation w.r.t the distribution of Y :

$$H(X|Y) = - \sum_{x,y} \Pr[X = x, Y = y] \log_2(\Pr[X = x|Y = y])$$

Proof of OTP security

Statement

X : cleartext.

Y : ciphertext.

K : key.

We want to show:

$$H(X|Y) = H(X)$$

Proof of OTP security

Proof

$$\begin{aligned}\Pr[X = x, Y = y] &= \Pr[X = x, K = x \oplus y] \\ &= \Pr[X = x] \times \Pr[K = x \oplus y] \\ &= \Pr[X = x] \times 2^{-n}\end{aligned}$$

Sum over all x :

$$\Pr[Y = y] = 2^{-n}$$

Finally,

$$\Pr[X = x | Y = y] = \frac{\Pr[X=x, Y=y]}{\Pr[Y=y]} = \frac{\Pr[X=x] \times 2^{-n}}{2^{-n}} = \Pr[X = x].$$

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 $c = c_1c_2 \cdots c_t$ 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

▶ $C = \text{Aduaenttlydhatoiekounletmtoihahvsekeeeleeyqonouv}$

Example: transposition ciphers

- $C = \text{Aduaenttlydhatoiekounletmtoihahvsekeeeleyqonouv}$

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 $1, \dots, 50$.

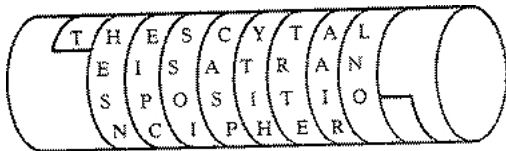
Example: transposition ciphers

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

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

It is good to use Confusion and Diffusion together

Outline

Presentation

Motivations

History of Cryptography

Exercises

Challenge

Conclusion

Overview

Decrypt the following ciphers (they all correspond to an encryption method seen in class):

1. (very easy) 20-8-5-13-15-19-20-9-13-16-15-18-20-1-14-20-20-8-9-14-7-9-14-3-15-13-13-21-14-9-3-1-20-9-15-14-9-19-20-15-8-5-1-18-23-8-1-20-9-19-14-20-2-5-9-14-7-19-1-9-4
2. (easy) FDWV DUH LQWHQGHG WR WHOO XV WKDW QRW HYHUBWKLQJ LQ QDWXUH KDV D IXQFWLRQ.
(Hint: B.C.)
3. (medium) OUFWIY ATNHAT DONNIG GHRTEI TYOODI ELRFUS
(Hint: observe the structure of the ciphertext)
4. (hard) JF CFEX REU KYREBJ WFI RCC KYV WZJY
(Hint: ROT-*N*)
5. (hard)

ESIRNDVYIUPEOGCRDFNAOIYOTGSORIRCUAOEORNNSVOCISEWE

(Hint: The cipher has 50 letters)

Churchyard cipher



► **History:**

- This ciphertext appeared engraved on a tombstone in Trinity Churchyard (New York) in 1794.
- First published solution: 1896.

► **Questions:**

1. What kind of cipher is it?
2. Why is it so difficult to break? (Especially without the hint!)
3. What is the plaintext message?
4. What is the key?

► **HINT: TIC TAC TOE =**



Outline

Presentation

Motivations

History of Cryptography

Exercises

Challenge

Conclusion

Rules

- ▶ Decrypt the text online on the Web site
- ▶ Each week one hint until somebody finds it.
- ▶ I will put the name online of the first winner.
- ▶ Use everything you need.
- ▶ To win explain how you did to solve it.

Encoded Message:

pf dgs nojsb yykx hvxlxtgu xg zye syuk nxoxj dm vyc gwtvtllvy rxbzlrn rjrr mvoj lvpnu ltg sexue nyivvku zlcpw tbj
cavqgcw um znijnlzetgqkj vyckcg hnrn typj pgr pei yu kdkhgc pz jqz hkt twhr rq fst bjzggg iassjeaccu yqhiz twlgt
tpkwuls jmptcggg khtf yvpt giiuipkjc otu hasfzcs dkihpwq rjbhgz ah lci dpze ah y dyc kokh h ozaghgifpt kxkfi
giiuipkjc mvk tghluzccm iiepastvq mvvgk hdytd pgr duaagrcw bb r symr mu kgkeg ukkf bblznxac tmbizgtecjw dcc
kkt am rls txf dcct rwbg xldic rzdnh khtpp cgimzk aumyqi q lsvnt gp rwxwx ahzstrlx uw iocki tfdoie vtgi bthzvr
pr zq icyjiqsc kfpm zye plhlqdkwg uckct rwx szcgvqefnt ru twl urkt bu ocl irtt o khdbejk ih zye vjfv pxcxdh mh
qetqk ah qqlprxg ff osorl wotxeg mt rwhimyt vd kftf ueln rq bxlaojs afg gsxo ff sghv jict twlk rq bavfshpznv dk
odpgvzcsjt wz ih awigdng ko ycerja gude vd kft aketps jrxxmg ff afqjc wsvrrilb uynl gk bvqv rtkfkjtgpy n ktg lnrpfc
rwxfk mxnfv zt czyeg kge jict mpyq gcgaovj xudgigdk zf iocjoaosity ack tvysr zf lljefkt o dihzgqeygr kettyntzqt mkk
pjqjq mvk gjsd fd ldgte tgpuq mvvgk pyc km hix mxubu yh cais hpg rd hnfst mh rwx hvahaq kfpm vrxzf zlixzrvicz
xrqi otu rvmn ycw aesntnckftmwi rnytu cs hnzs lytkf pwzy tutkfs h sevs hlf qahkrp pub jsgxze dglu kftbf glpuq
repbyk jz ceb xoxcy pl kft hcvnipcvy rxbzlrn acdc mvk gglyv bxlwrcuhpmpdccc neas ffit vcepzc jccw ziyh qqsibct
td ncjape rrfdbperbt

Outline

Presentation

Motivations

History of Cryptography

Exercises

Challenge

Conclusion

Summary

Today

- ▶ Presentation
- ▶ Motivation
- ▶ History of Cryptography

Next Time

- ▶ Classical Symmetric Encryption

Thank you for your attention



Questions ?

Solutions 1

20-8-5-13-15-19-20-9-13-16-15-18-20-1-14-20-20-8-9-14-
 7-9-14-3-15-13-13-21-14-9-3-1-20-9-15-14-9-19-20-15-8-
 5-1-18-23-8-1-20-9-19-14-20-2-5-9-14-7-19-1-9-4

Each letter has been replaced by its rank in the alphabet:

*THEMOSTIMPORTANTTHINGINCOMMUNIC
 ATIONISTOHEARWHATISNTBEINGSAID*

And we add spaces:

*THE MOST IMPORTANT THING IN
 COMMUNICATION IS TO HEAR WHAT ISN T BEING
 SAID*

Solutions 2

*FDWV DUH LQWHQGHHG WR WHOO XV WKDW
QRW HYHUBWKLQJ LQ QDWXUH KDV D
IXQFWLRQ.*

This is Caesar cipher: to decrypt it, we replace each letter with the character three to the left modulo 26:

*CATS ARE INTENDED TO TELL US THAT NOT
EVERYTHING IN NATURE HAS A FUNCTION.*

Solutions 3

*OUFWIY ATNHAT DONNIG GHRTEI TYOODI
ELRFUS*

This is a permutation cipher with block length 6. The permutation is $\begin{pmatrix} 123456 \\ 536124 \end{pmatrix}$ and the plaintext is:

*IFYOUW ANTATH INGDON ERIGHT DOITYO
URSELF*

or with proper word breaks:

*IF YOU WANT A THING DONE RIGHT DO IT
YOURSELF*

Solutions 4

JF CFEX REU KYREBJ WFI RCC KYV WZJY

This is encoded using ROT-17. The plaintext is:

SO LONG AND THANKS FOR ALL THE FISH

Solutions 5

ESIRND VYIUPEOGCRDFNAOIYOTGSRIRC UAEOERNNSVOCIS

This is a transposition cipher, it has 50 characters. We write them in a square of 5x10 characters, from left to right and then from top to bottom:

E	S	I	R	N
D	A	V	Y	I
U	P	E	O	G
C	R	D	F	N
A	O	I	Y	O
T	G	S	O	R
I	R	C	U	A
O	E	O	R	N
N	S	V	O	C
I	S	E	W	E

We now read it from top to bottom and then from left to right:

Solutions

1. Substitution.
2. Not enough cipher text to perform a frequency analysis.
3. REMEMBER DEATH
4. The substitution is designed by this scheme:

A	B	C
D	E	F
G	H	I

J	K	L
M	N	O
P	Q	R

S	T	U
V	W	X
Y	Z	

Thank you for your attention



Questions ?