Códigos y Criptografía

Francisco Rodríguez Henríquez
CINVESTAV
francisco@cs.cinvestav.mx

Anuncios Importantes (1/2)

- Implementaciones de algunos de los algoritmos criptográficos que serán estudiados en este curso pueden encontrarse en:

  www.prenhall.com/washington

  Dichas implementaciones están escritas en MatLab, Maple y Mathematica.

- Libro de texto

  "Introduction to Cryptography with Coding Theory",

  W. Trappe & L.C Washington,

  Prentice-Hall, 2002. ISBN:0-13-061814-4.

Anuncios Importantes (2/2)

- 2 exámenes parciales (30%)
- 4 tareas (40%)
- Proyecto final (30%)
- Quizzes (10%)

Las fechas de los exámenes, tareas y proyectos finales serán anunciados en la próxima clase así como en el portal internet de la clase.

Especificaciones del Proyecto Final (1/2)

Las especificaciones generales del proyecto son:

- Seleccionar un método criptográfico a desarrollar, investigando en la literatura especializada (Internet, libros, reportes técnicos y artículos).
- Seleccionar el lenguaje de programación (y correspondiente plataforma) que se utilizará en el desarrollo del proyecto. Ejemplos: C, C++, MatLab, Maple, Java, VHDL, etc.
- El proyecto deberá incluir un método razonable de verificación de los resultados producidos. Por ejemplo, típicamente en los diferentes estándares de criptografía se incluyen vectores de prueba (dado un vector de entrada obtener el correspondiente vector de salida).

Especificaciones del Proyecto Final (2/2)

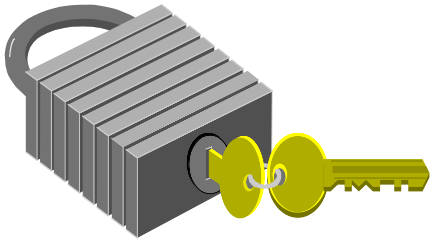
- El proyecto deberá contar con un ejemplo a manera de “demo” de tal manera que su uso pueda ser fácilmente comprendido por el resto de la clase. Tanto el reporte final del proyecto como la implementación del mismo serán incluidos en el portal internet del curso.
- Las fechas para proponer un tema de proyecto así como la fecha para la entrega final del mismo serán dadas a conocer en la siguiente clase.

Outline

- Importance of cryptography
- A Brief History of Cryptography
- Cryptography Greatest hits
- Basic Concepts
- Security Threats & Attacks
- Classes of Security Attacks
- Security Services
- Some practical applications
- Some Research Interests in Cryptography
- Cryptography Schemes

Why Security?

- Information is a strategic resource. As information super-highways are developed, cryptographic techniques are needed for privacy and authentication of digital data.
- The vast majority of digital information is both, stored and processed within a computer and transferred between computers.
- Some of the requirements for security must consider/prevent
  - threats and possible attacks to information's security
  - mechanisms to detect, prevent or recover from attacks
  - services which enhance security



A Brief History of Cryptography

- Ancient Ciphers have a history of at least 4000 years.
  - Ancient Egyptians enciphered some of their hieroglyphic writing on monuments
  - ancient Hebrews enciphered certain words in the scriptures
  - 2000 years ago Julius Ceasar used a simple substitution cipher, now known as the Caesar cipher
  - Roger Bacon described several methods in 1200s
  - Leon Alberti devised a cipher wheel, and described the principles of frequency analysis in the 1460s
  - Blaise de Vigenère published a book on cryptology in 1585, and described the polyalphabetic substitution cipher

increasing use, especially in diplomacy & war over centuries

Hieroglyphic encipherments of proper names and titles, with cipher hieroglyphs at left, plain equivalents at right

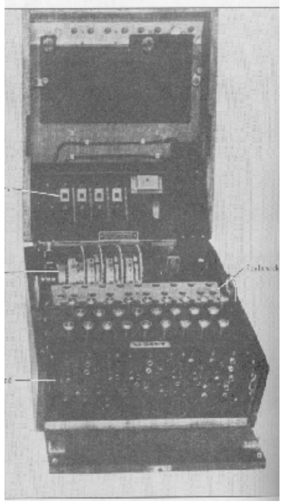
Cryptography Greatest hits: The Rosetta Stone

- From 452 to 1822, "Egypt was silent”: The ability to read hieroglyphic inscriptions on monuments and tombs, and papyrus texts using cursive scripts like demotic, was lost. However, the spoken language itself survived, using Greek letters plus 7 signs derived from demotic, as the Coptic language.
- The Rosetta Stone was discovered in July, 1799, while some of Napoleon's troops were demolishing ancient structures to make way for a fort.
- (http://www.cs.oberlin.edu/classes/cs115/lect29n.html)

The Rosetta Stone, with Egyptian hieroglyphics in the top section, demotic characters in the middle, and Greek at the bottom; in the British Museum.

Cryptography Greatest hits: Enigma

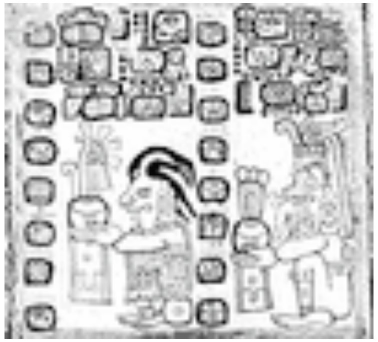
- Enigma: Device used by the German military command to encode strategic messages before and during World War II. The Enigma code was broken by a British intelligence system known as *Ultra*.
- A British cryptographer smuggled a complete new Enigma machine to England. There, British mathematicians and cryptographers conquered the problems of Enigma variations and found means of cracking the ciphers. Alan Turing played a significant role in breaking the German "Enigma" codes.



Cryptography Greatest hits: Mayan writing system

- System of writing used by the people of the Mayan Indian civilization of Meso-America from about the 3rd century AD until about the end of the 17th century, 200 years after the Spanish conquest of Mexico.
- It was the only true writing system developed in the pre-Columbian Americas. Mayan inscriptions are found on *estelas* (standing stone slabs), stone lintels, sculpture, and pottery, as well as on the few surviving Mayan books, or codices.
- The Mayan system of writing contains more than 800 characters, many of which are hieroglyphic; i.e., they are recognizable pictures of real objects.
- During the 1950s the linguist Yury Knorozov demonstrated that the Mayan writing system contained both logograms and phonetic signs representing syllables.

The corn god and the rain god, Chac. Drawing from el códice Madrid (Codex Tro-Cortesianus), one of the Mayan sacred books.



Cryptography Greatest hits: The gold-bug

```
53++!305))6*;4826)4+.)4+);806*;48!8`60))85;]8*:+*8!83(88)5*!;
  46(;88*96*?;8)*+(;485);5*!2:*+(;4956*2(5*-4)8`8*; 4069285);)6
  !8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?3
  4;48)4+;161;:188;+?;
```

Ciphertext

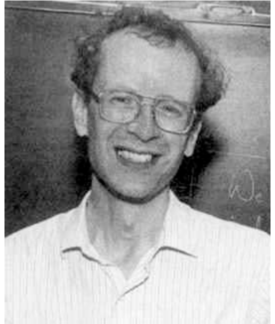
'A good glass in the bishop's hostel in the devil's seat twenty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee line from the tree through the shot fifty feet out.'

Plaintext

Edgar Allan Poe (1809-1849)

Cryptography Greatest hits: Fermat’s last theorem

- Also called Fermat’s great theorem, the statement that there are no natural numbers x, y, and z such that $x^n + y^n = z^n$, in which n is a natural number greater than 2. About this the 17th-century mathematician Pierre Fermat wrote in 1637 in his copy of Claude-Gaspar Bachet's translation of Diophantus' Arithmetica, *"I have discovered a truly remarkable proof but this margin is too small to contain it."* Mathematicians long were baffled by the statement, for they were unable either to prove or to disprove it, although the statement had been proved for many specific values of n.
- Using Elliptic curve theory, the English mathematician Andrew Wiles, with help from his former student, Richard Taylor, devised a proof of Fermat's last theorem that was published in 1995 in the journal Annals of Mathematics. For an excellent summary of the tries for proving the theorem, see http://wwwgroups.dcs.stand.ac.uk/~history/HistTopics/Fermat's_last_theorem.html.

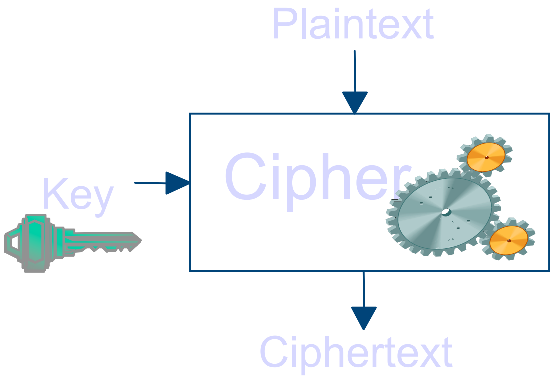


http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Wiles.html

$F(n) = 2^{2^n}+1$

Basic Concepts

- ***Cryptography***. - The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then re-transforming that message back to its original form
- ***Plaintext***.- The original intelligible message
- ***Ciphertext*** .- The transformed message
- ***Cipher***.- An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods
- ***Key.-*** Some critical information used by the cipher, known only to the sender & receiver
- ***Cryptanalysis***.- The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called codebreaking



Security Threats & Attacks

Threats can come from a range of sources, with results of order:

- 55% human error
- 10% disgruntled employees
- 10% dishonest employees
- 10% outsider access
- By accident/incident (fire, flood etc)