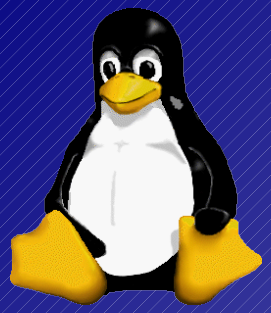
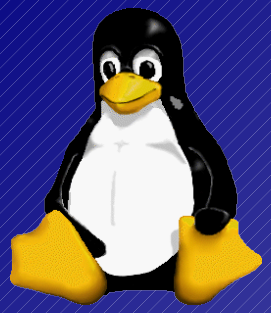
Cryptography Basics

A History of Cryptography



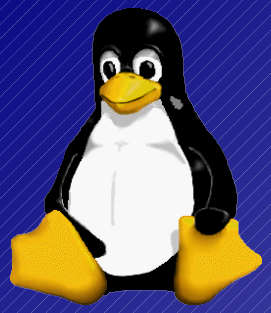
Ancient

- around 1900 B.C., Egypt
  - tomb inscriptions used unusual forms of hieroglyphs to make the text look more important
- 500-600 B.C., Israel
  - a version of the book of Jeremia is written using a reverse alphabet
- 50-60 B.C., Rome
  - Julius Caesar uses shifted alphabets (Caesar Cyphers)



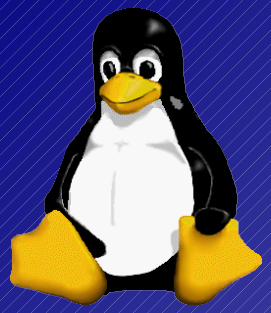
Arabic

- 725-790 Abu `Abd al-Rahman al-Khalil ibn Ahmad ibn `Amr ibn Tammam al Farahidi al-Zadi al Yahmadi
  - writes a book about basic statistical analysis of encrypted text
- 855 Abu Bakr Ahmad ben `Ali ben Wahshiyya an-Nabati
  - publishes several common cypher alphabets



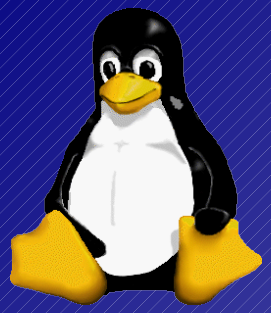
Europe, middle age

- between governments and their ambassadors it is common to communicate in cyphers (normally simple caesar cyphers or similar)
- ca. 1466, Leon Battista Alberti invented the polyalphabetic cypher
- 1553, Giovan Batista Belaso invents keyed cyphers
- 1585, Blaise de Vigenère betters the Belaso system by making each letter part of the key for the next letter



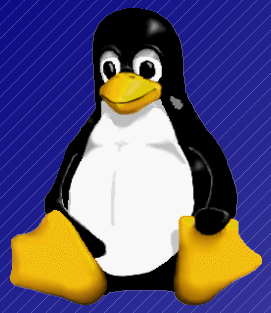
Northern America

- 1790's, Thomas Jefferson invents the wheel cypher
- cyphers were used on both sides in the civil war
- 1854, Charles Wheatstone & Lyon Playfair invent the “Playfair cypher”
- 1929, Lester S. Hill starts using algebraic cyphers



WorldWar II

- Germany: Enigma
  - was broken by Polish mathematician Marian Rejewski
  - further brakings by Alan Turing, Gordon Welchman
- Japan: purple machine
  - broken by William Frederick Friedman
- U.S.A.: SIGABA
  - invented by William Frederick Friedman



Modern

- 1970, Dr. Horst Feistel (at IBM)
  - invents the Lucifer cypher, which lead to:
- 1976, IBM
  - DES is chosen as NSA's standard
- 1976, Whitfield Diffie and Martin Hellman
  - introduce the idea of public key cryptography
- 1977, Ronald L. Rivest, Adi Shamir and Leonard M. Adleman
  - introduce RSA algorithm

Questions?

?