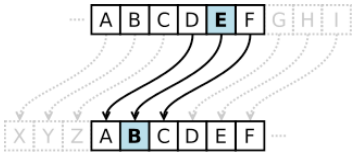
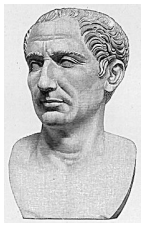
Cryptography Overview

CSCI 10 - Santa Clara University - Fall 2017
Michael J. Bannister

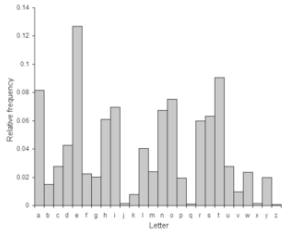
Caesar Cipher



Shifts each letter by a fixed amount



Named after Julius Caesar



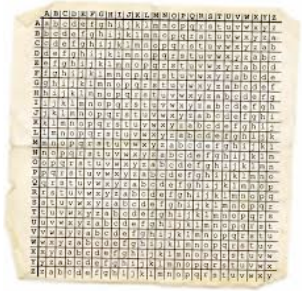
Vulnerable to Stat Analysis

Caesar Cipher

- Key can be thought of as a single character.
- Only 26 possible keys in english!
- Does not change frequency distribution

Vigenère Cipher

Named for Blaise de Vigenère

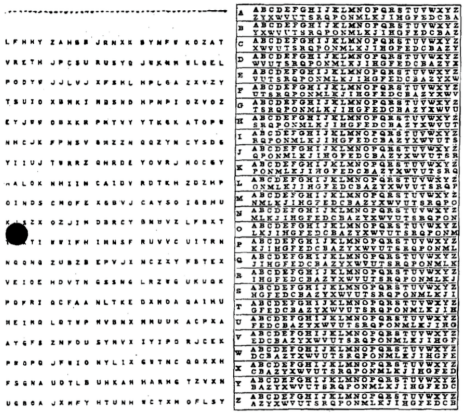


Different Caesar ciphers based on position

Vigenère Cipher

- Keys are multi-character words
- Essentially unlimited number of keys
- Changes frequency distribution
- Still vulnerable to statistical attack if key is short relative to message length.

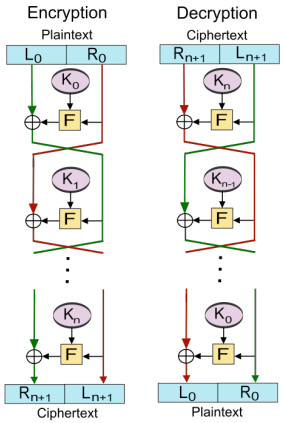
One-Time Pad



NSA one-time pad

- Vigenère with key size equal to message size
- Key must be random
- Can only be used once
- Perfectly secure
- Massive key keep/store

Modern Symmetric-Key Encryption



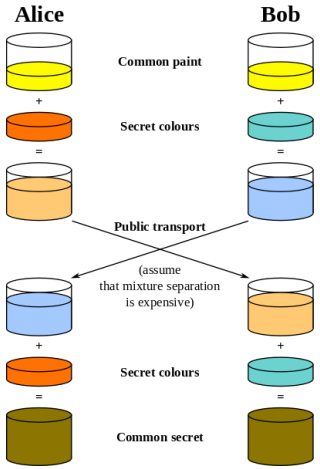
Feistel Networks

Horst Feistel (1915-1990)

Modern Symmetric-Key Encryption

- Keys are bit strings
- Typically keys are 128 to 256 bits
- Destroys frequency distribution; small change in the input yield dramatic change in the output
- Very fast and very secure; What protects secure web pages.
- Need to agree on a secret key!

Secure Key Exchange



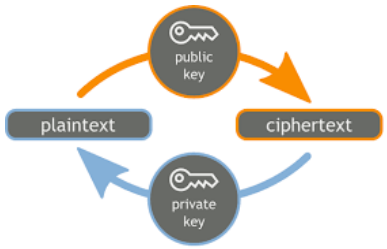
Whitfield Diffie

Martin Hellman

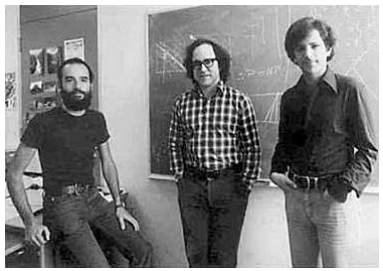
Logjam Attack

- Security vulnerability in DH key exchange implementations
- Most internet traffic is secured using the same *common paint*
- Estimated to cost a "few hundred million dollars" to build hardware that can break one *common paint* per year
- The security community believes the NSA has used this method to spy on large percentage of internet traffic
- Conclusion: we can't all use the same *common pain*

Public-Key Cryptography



Creators of RSA



Adi Shamir, Ron Rivest, Leonard Aldeman

Public-Key Cryptography

- Asymmetric key! The encryption and decryption key are different and it is difficult to convert one to the other.
- Typically keys are ~2000-4000 bits
- Very secure, but slow compared to symmetric
- Good for email and other non-real time communication
- Can be used to verify identity

Legality (USA)

- Export controlled and classified as a munition
- Daniel J. Bernstein through a set of court cases argued that printed source code was protected under free speach
- Philip Zimmermann exported PGP by exporting the printed source code, which was then re-typed and compiled outside the US.
- Currently governments around the world are trying to required that all cryptographic software have government master key.

Government Access Debate

Extra Credit

Be subversive and send me an encrypted email! You can find my PGP public key on webpage, and you can learn how to use it by googling "how to send a PGP email".

Please include you name in the message.

Worth 5 points toward your homework grade!