Transposition (strip of paper wrapped around a staff)
Substitution (Caesar cipher)

Caesar Cipher → brute force or frequency analysis
Substitution cipher → frequency analysis
Viginere cipher → index of coincidence
One-time-pad is theoretically unbreakable
– Malleability is a concern

Little bit of history (Enigma, Turing, Freidman)
– See David Kahne's *Codebreakers*

Kerckhoffs' Principles (1883):

1. The system must be practically, if not mathematically, indecipherable
2. It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience
3. Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents
4. It must be applicable to telegraphic correspondence
5. It must be portable, and its usage and function must not require the concourse of several people
6. Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

Data Encryption Standard (DES) – 1976

– 64-bit cipher; 56-bit key; 16 round Feistel structure

Advanced Encryption Standard (AES) – 2001

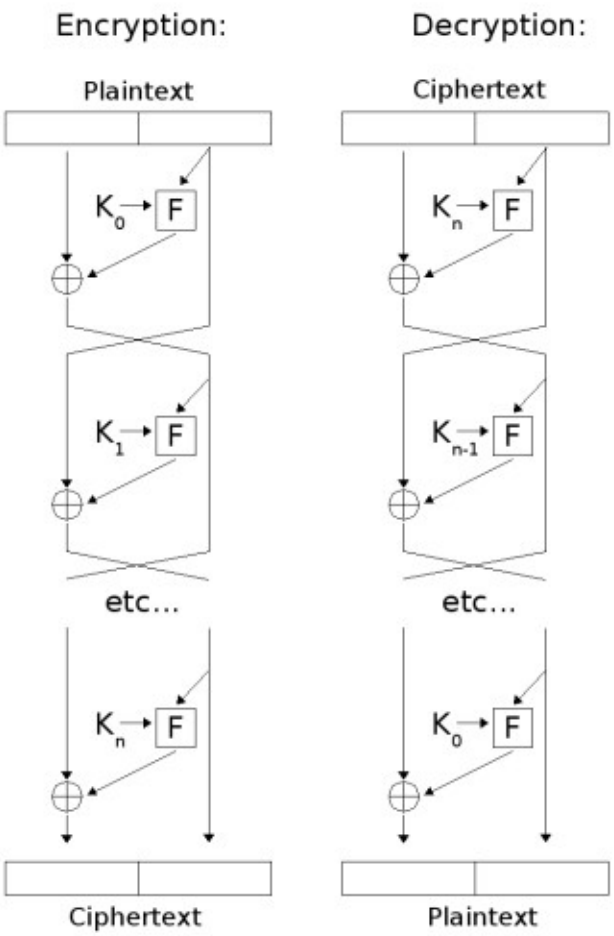
- 128-bit cipher; 128, 192-, or 256-bit key; 10, 12, or 14 rounds
- Substitution Permutation Network

Known plaintext vs. chosen plaintext vs. ciphertext-only attacks

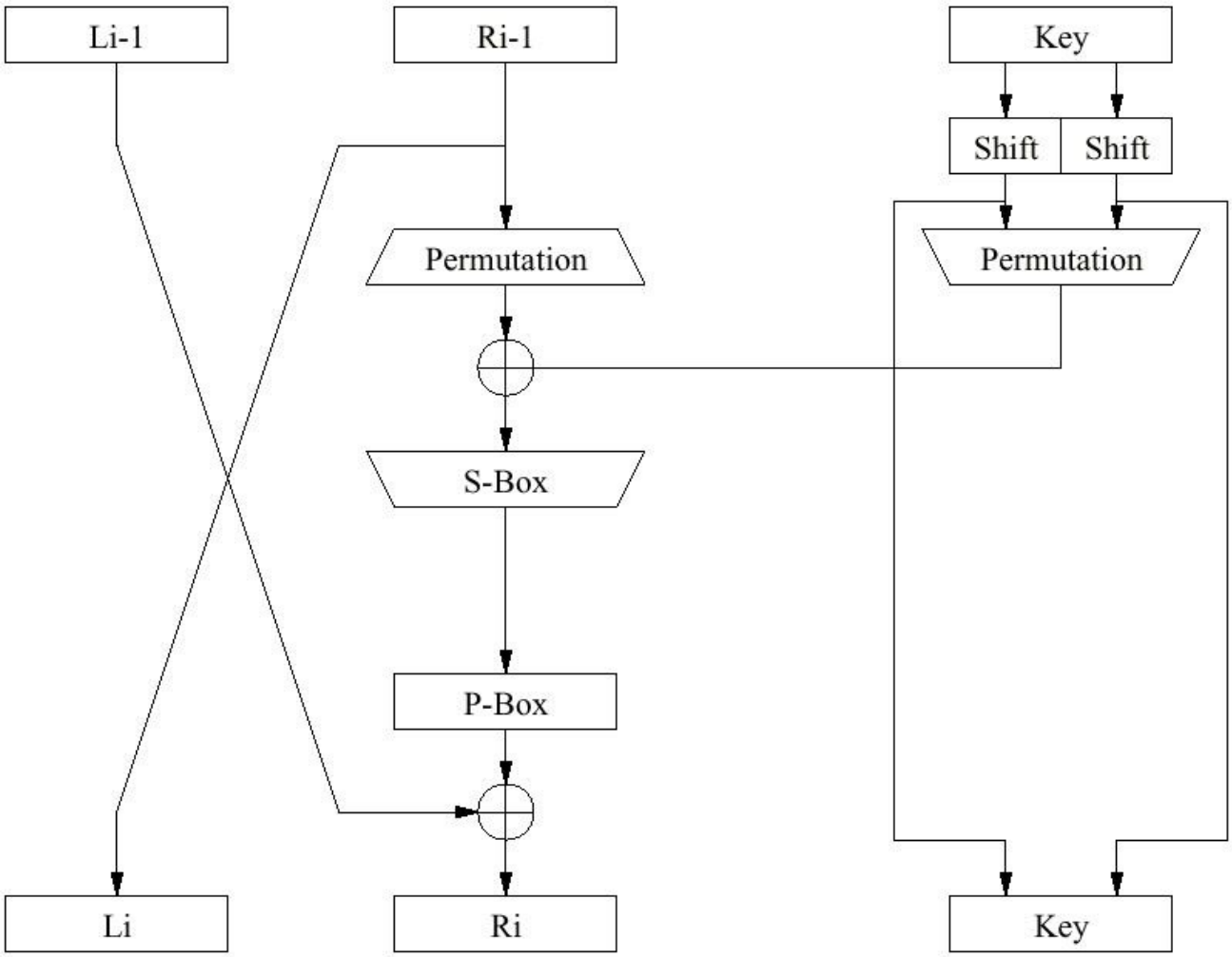
Known plaintext example: linear cryptanalysis
Chosen plaintext example: differential cryptanalysis
Cipher-text only example: Examples above for Caeser cipher, etc.

Cryptographic hash

See WEP attacks on page 436 of “Hacking: the Art of Exploitation”
Stream ciphers and related-key attacks: (A xor C) xor (B xor C) = A xor B
Birthday paradox: 1-e^(-(54*54)/2*365)) = 0.98...
20: 41.1%, 23: 50.7%, 30: 70.6%, 50: 97%



Feistel Cipher


Li-1
Ri-1
Key
Shift
Shift
Permutation
Permutation
S-Box
P-Box
Li
Ri
Key

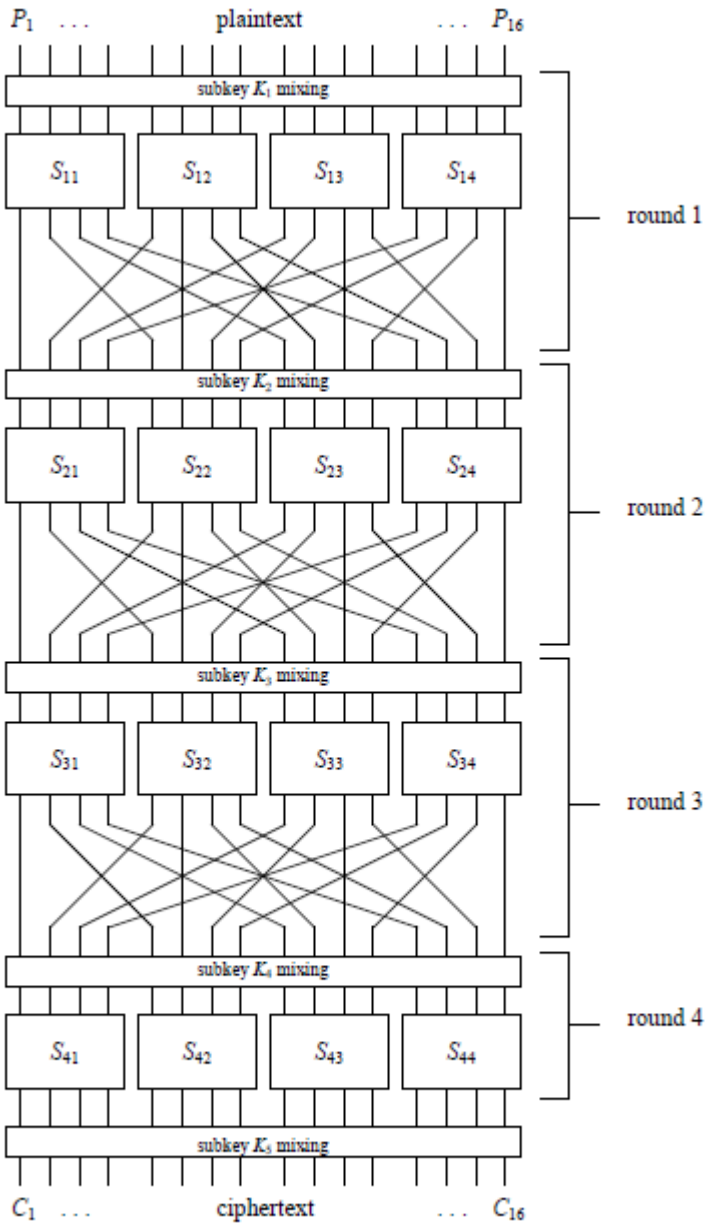
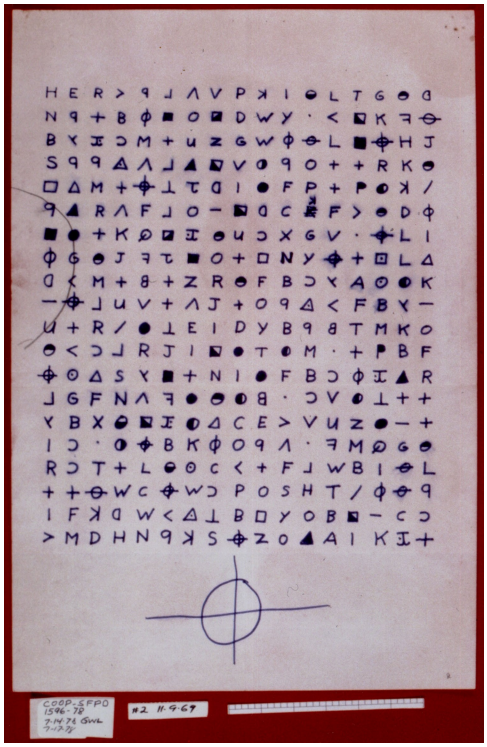


Figure 1. Basic Substitution-Permutation Network (SPN) Cipher


COOP-SFPO
1596-78
#2 11-9-67

Public key cryptography, asymmetric encryption

Terminology: Key exchange, assymetric encryption, digital signature, non-reputability, threshold cryptography, ring signatures, identity-based encryption, cryptocounters, private information retrieval

Diffie-Hellman key exchange (1976) (don't forget Merkle)

- Alice has secret a, public p and g where p is prime and g is a primitive root mod p
- Bob has secret b
- Alice sends p and g to Bob
- Alice sends $A = g^a \bmod p$ to Bob
- Bob sends $B = g^b \bmod p$ to Alice
- Both calculate secret $s = A^b \bmod p = B^a \bmod p$

RSA

Quantum key distribution

Main takeway message: Quantum computation effectively breaks asymmetric cryptography, but not symmetric.