Exploration of Cryptography

Whitfield Diffie

Distinguished Visiting Professor

Zhejiang University

10 December 2020

Class 05
Post WWII
Block Ciphers
Key Management

Post World War II

Symmetric Cryptography

Stream ciphers gradually give way to block ciphers.

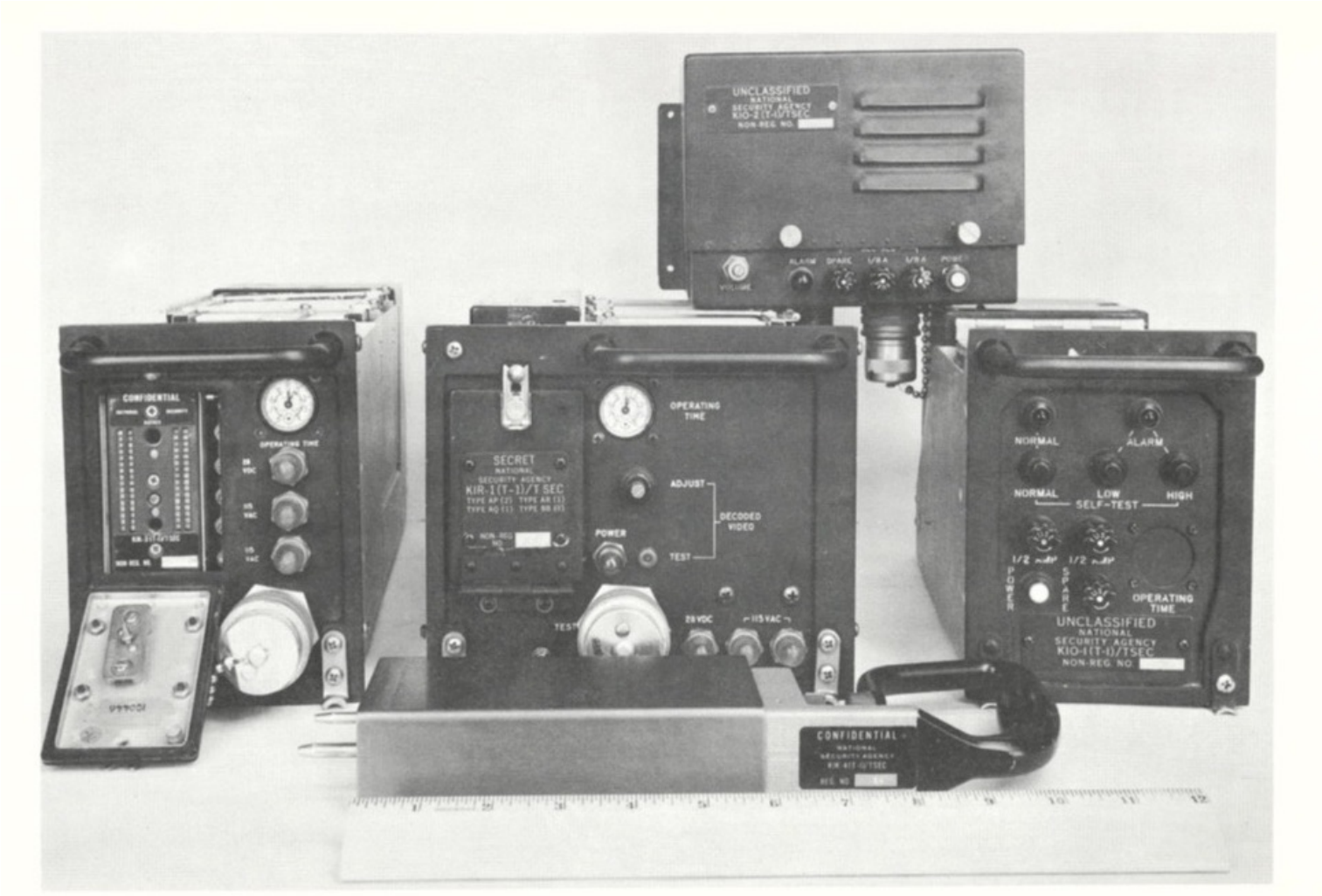
Identification Friend or Foe

- MK I to MK IX: analog
- MK X: digital but not crypto
- MK XII: encrypted

Identification Friend or Foe (Cont'd)

- Air Force Cambridge Research Center, early fifties
- System called Cadmus used in KI-1 used in MK XII
- 32-bit challenge, short response, done many times

KI-1


UNCLASSIFIED
NATIONAL SECURITY AGENCY
KIO-2(T-0)/TSEC
NON-REG. NO.
VOLUME
ALARM
SPARE
I/R A
I/R A
POWER
CONFIDENTIAL
OPERATING TIME
SECRET
NATIONAL SECURITY AGENCY
KIR-1(T-1)/T SEC
ADJUST
DECODED VIDEO
POWER
TEST
28 VDC
115 VAC
NORMAL
ALARM
NORMAL
LOW
HIGH
SELF-TEST
1/2 AMP
1/2 AMP
SQUELCH
VOLUME
OPERATING TIME
UNCLASSIFIED
NATIONAL SECURITY AGENCY
KIO-1(T-0)/TSEC
NON-REG. NO.
CONFIDENTIAL

Horst Feistel

IBM 2984 Banking System

- Feistel crypto design
- 32-bit block, 64-bit key
- Perhaps called DSD-1;
  now called AET

Things Called Lucifer

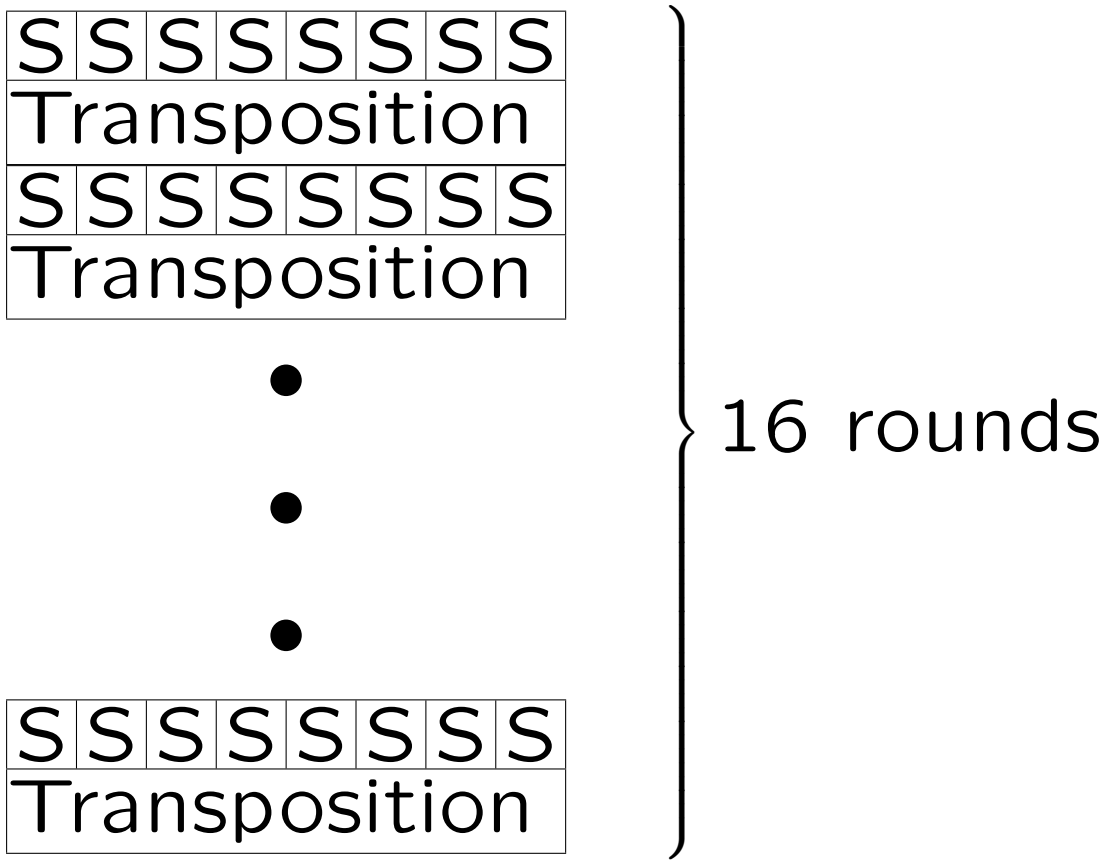
- Lucifer Box in 2984 (AET)
- Scientific American Lucifer
- Smith's Lucifer

Feistel Scientific American Article

Horst Feistel: "Cryptography and Computer Privacy" Scientific American, Vol. 228, No. 5, May 1973, pp. 15–23.

Abstract: Computer systems in general and personal "data banks" in need protection. This can be achieved by enciphering all material and authenticating the legitimate origin of any command to the computer.

Scientific American Lucifer



Scientific American Lucifer

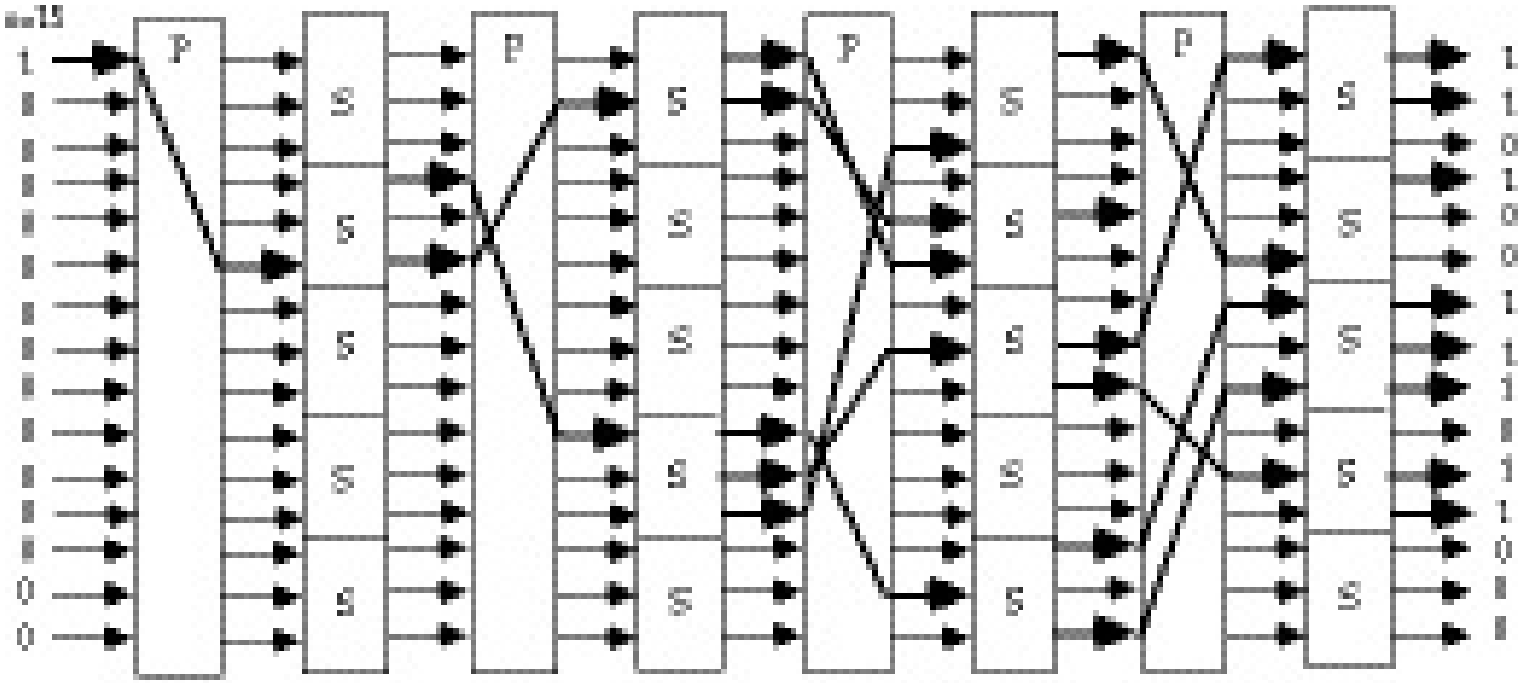


Fig 2.3 - Substitution-Permutation Network with the Avalanche Characteristic

Smith's Lucifer

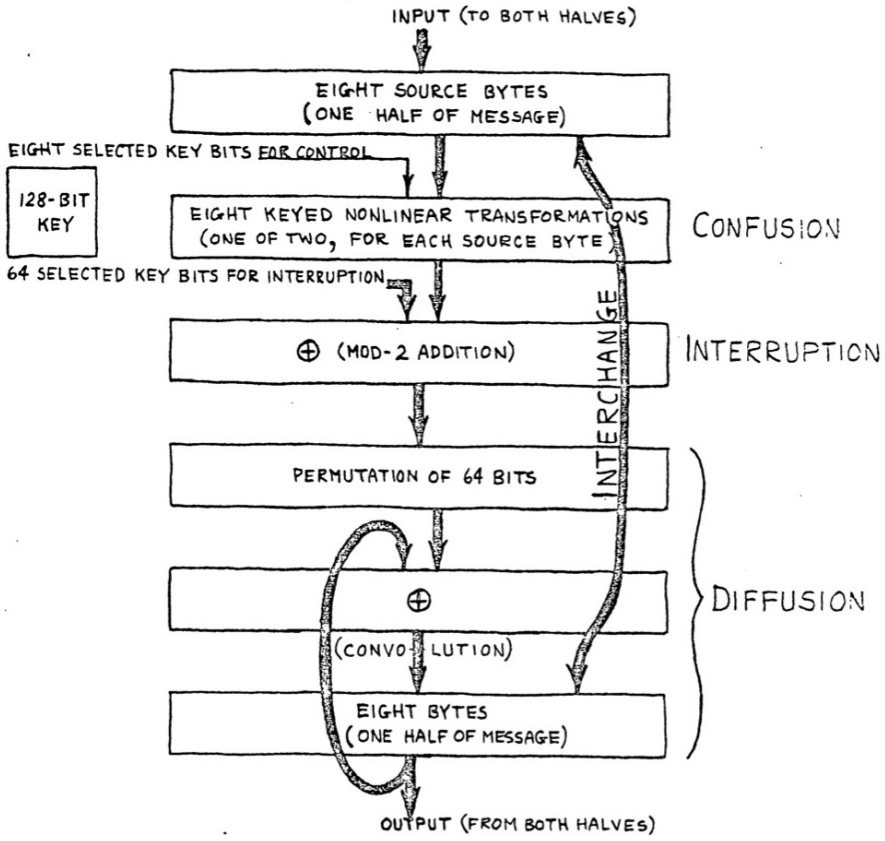
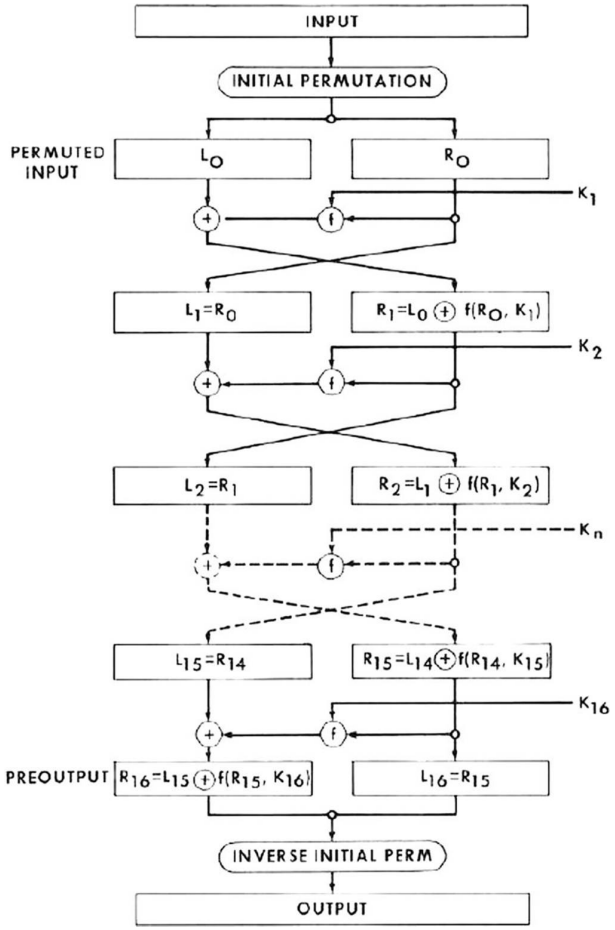


FIG. 1. FUNCTIONAL BLOCK DIAGRAM OF THE CIPHER SYSTEM

Data Encryption Standard

- Joint NSA-NBS project: 1973–1977
- Call for algs: IBM entry accepted
- 64-bit block, 56-bit key

Data Encryption Standard



Better Building Block

Block ciphers were recognized as a better building block than streams for diverse applications.

Blocks in the 1980s

- Various systems designed
- Elements of DES abstracted
- DES S-boxes studied

Nineties and On

- Differential cryptanalysis
- Linear cryptanalysis
- Broader understanding of block cryptanalyais

Nineties and On (Cont'd)

- DES $\Rightarrow$ 3DES
- Development of AES
- Other systems, mostly blocks

Development of AES

- Advanced Encryption Standard
- NIST Announcement of Contest
  — January 1997
- Two rounds of evaluation
- Fifteen applications accepted

Development of AES (Cont'd)

- Three big public meetings
  - Thousand Oaks California
  - Rome, Italy
  - New York, New York

Development of AES (Cont'd)

- Five finalists selected
  - Rijndael
  - RC6
  - Mars
  - Serpent
  - Twofish

Development of AES (Cont'd)

- Non-US design, Rijndael, chosen
- Truly, an international standard
- Standard adopted October 2001

Issues Today

- Internet of Things short on power
- Lookup tables use too much power
- Design for evaluation

Summary of Block Ciphers

- IFF Problem 1950s, Horst Feistel, Air Force Cambridge Research Center
- IBM "Lucifer" System for Lloyds Bank 1969
- DES 1975, 1977, and on
- AES 2001