Exploration of Cryptography

Whitfield Diffie

Distinguished Visiting Professor

Zhejiang University

27 March 2020

Class 04
Cryptography: Post WWII and Key Management

Grading

I would rather not grade but the University seems to want it.

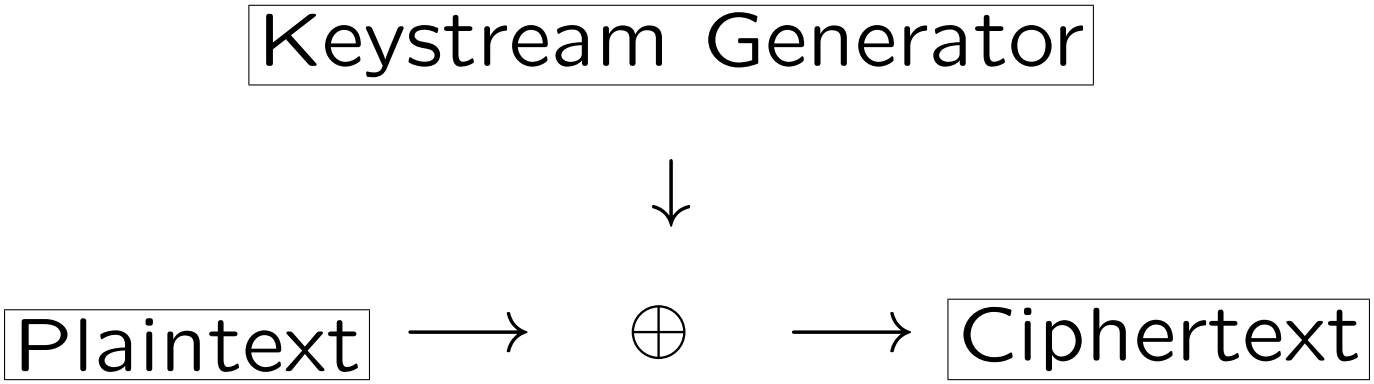
Two Problem Sets

• Midterm — next week due a week later

• Final — due late in course and due a week after you get it.

Beginning in WW II
Electronic Cryptosystems

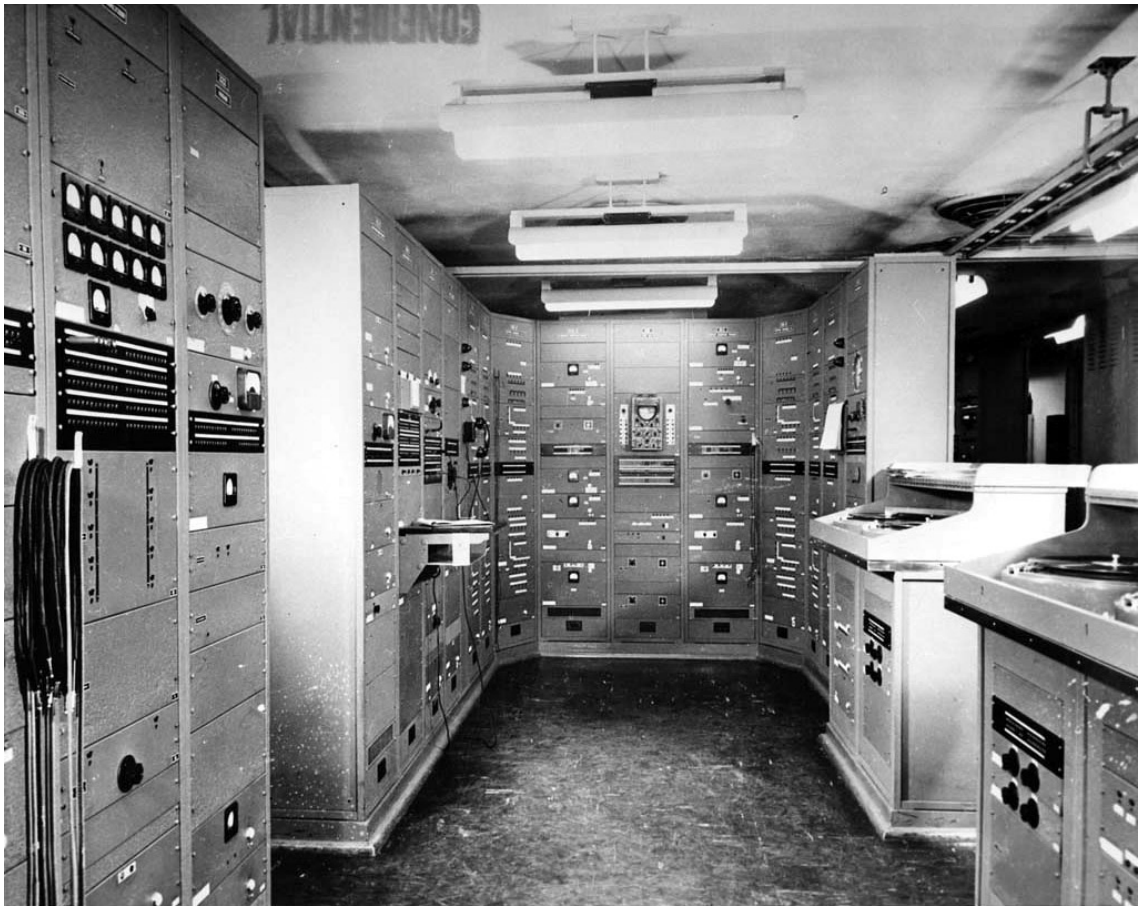
Stream Encryption



Keystream Generator Requirements

- Long period
- High Complexity

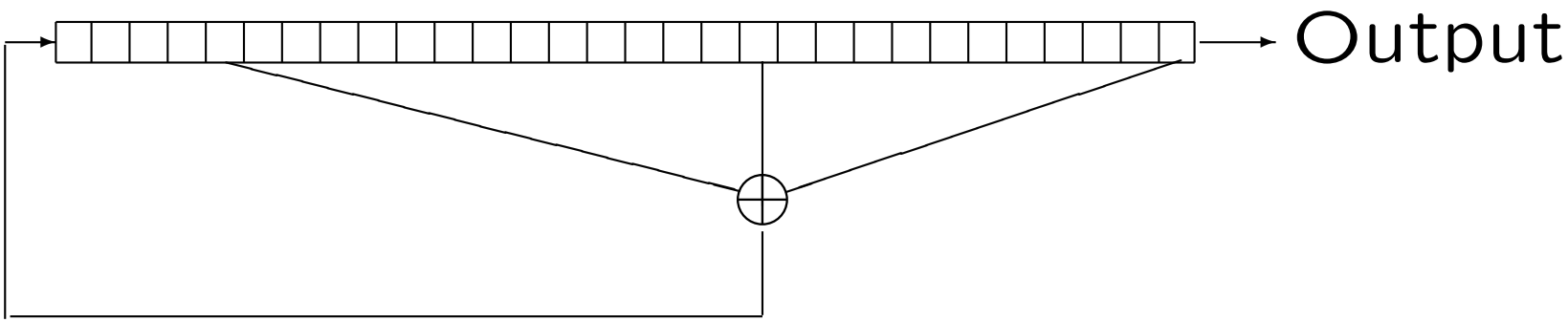
Sigsaly



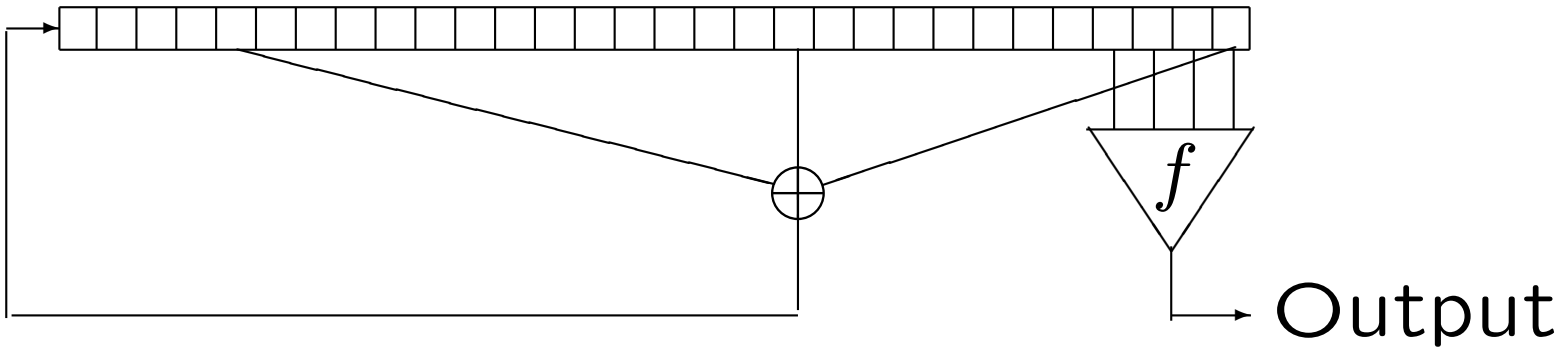
Long-cycle Systems

- Linear process, usually one or more shift registers
- Nonlinear combiner trees
- Irregular motion

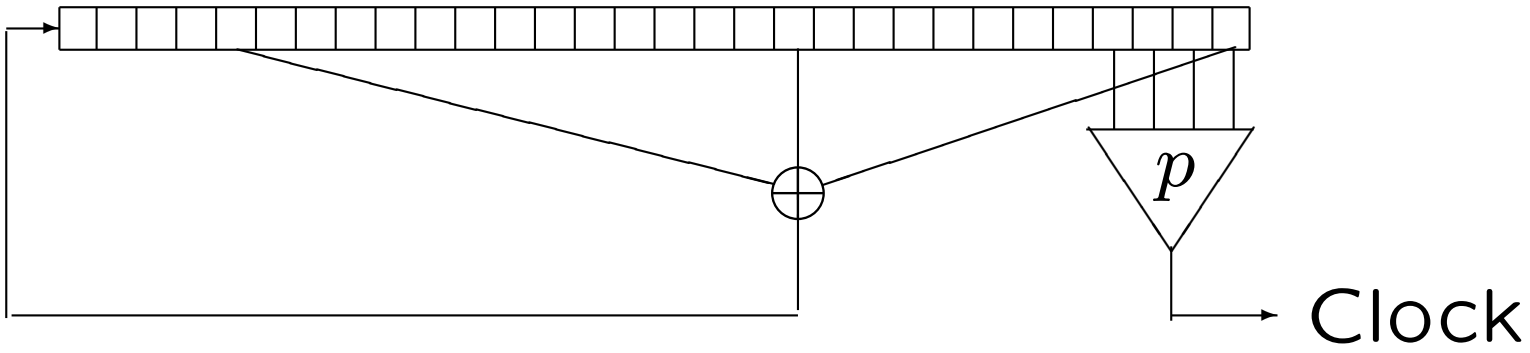
Linear Feedback Shift Register



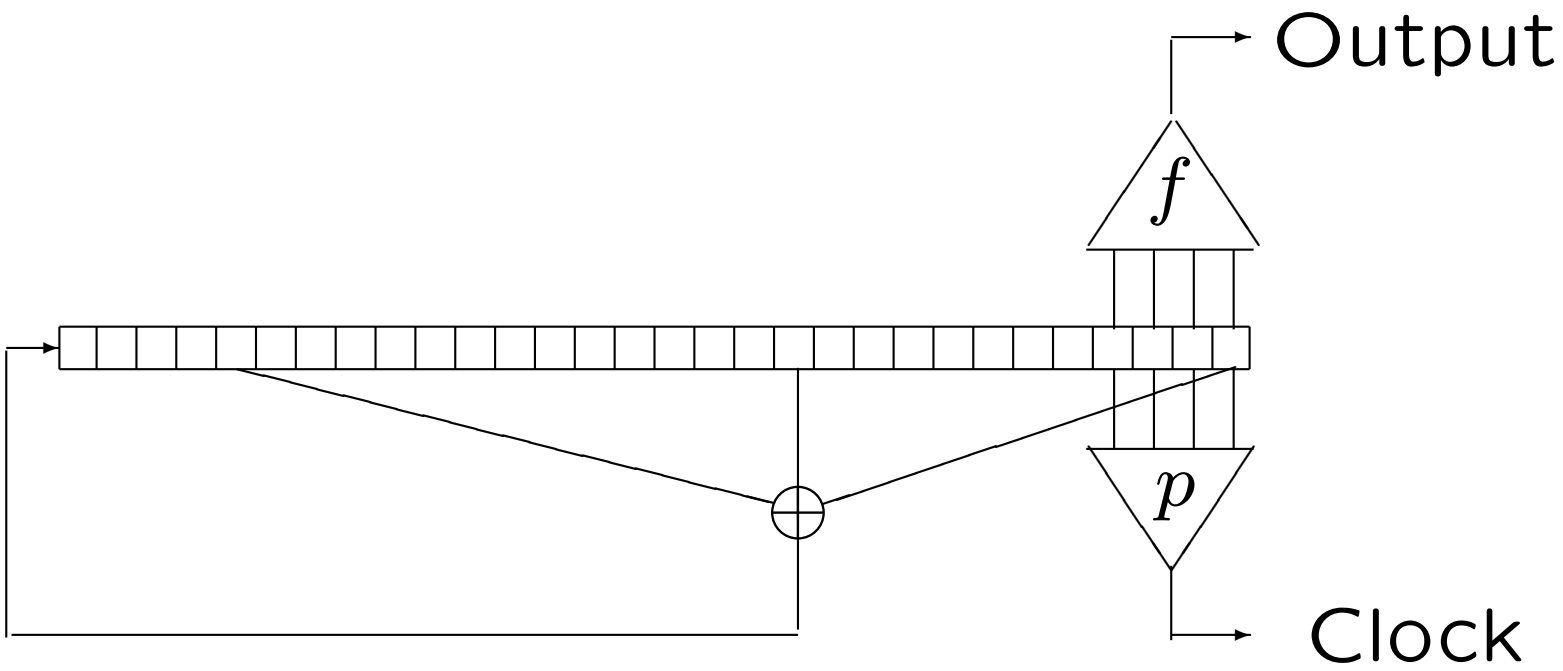
Linear Feedback Shift Register with Nonlinear Output



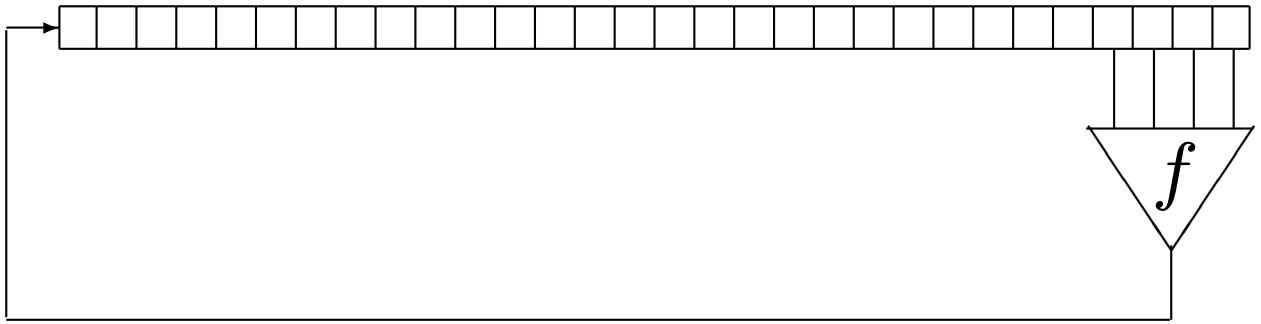
Linear Feedback Shift Register with Nonlinear Clocking



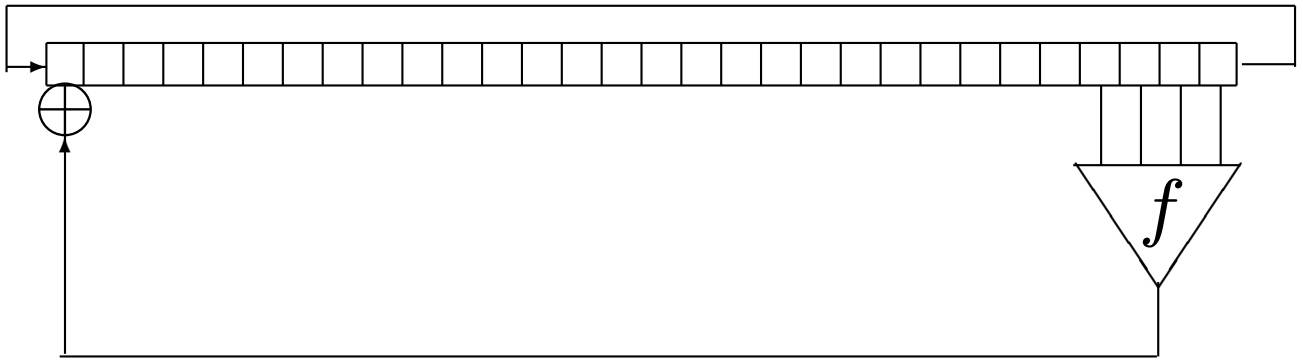
LFSR with Both



Nonlinear Feedback Shift Register

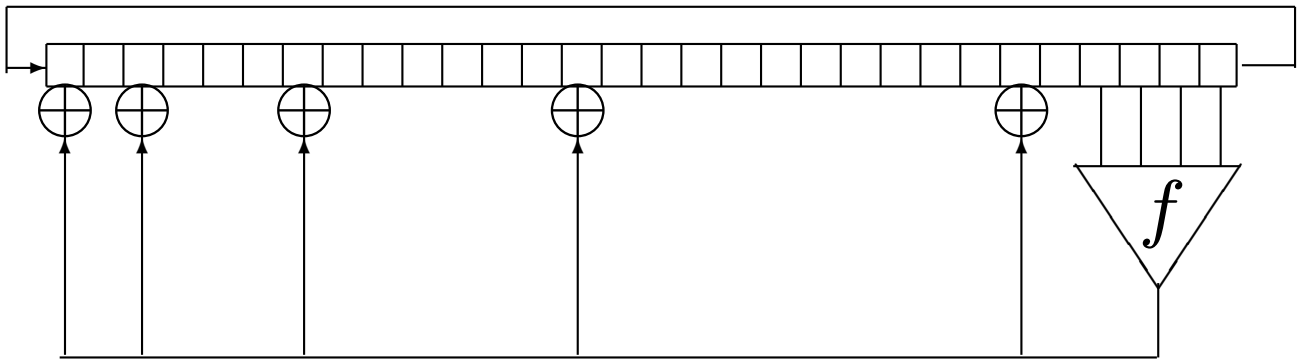


Invertible Shift Register Notation



Nonlinear Shift Register

with Multipoint Feedback



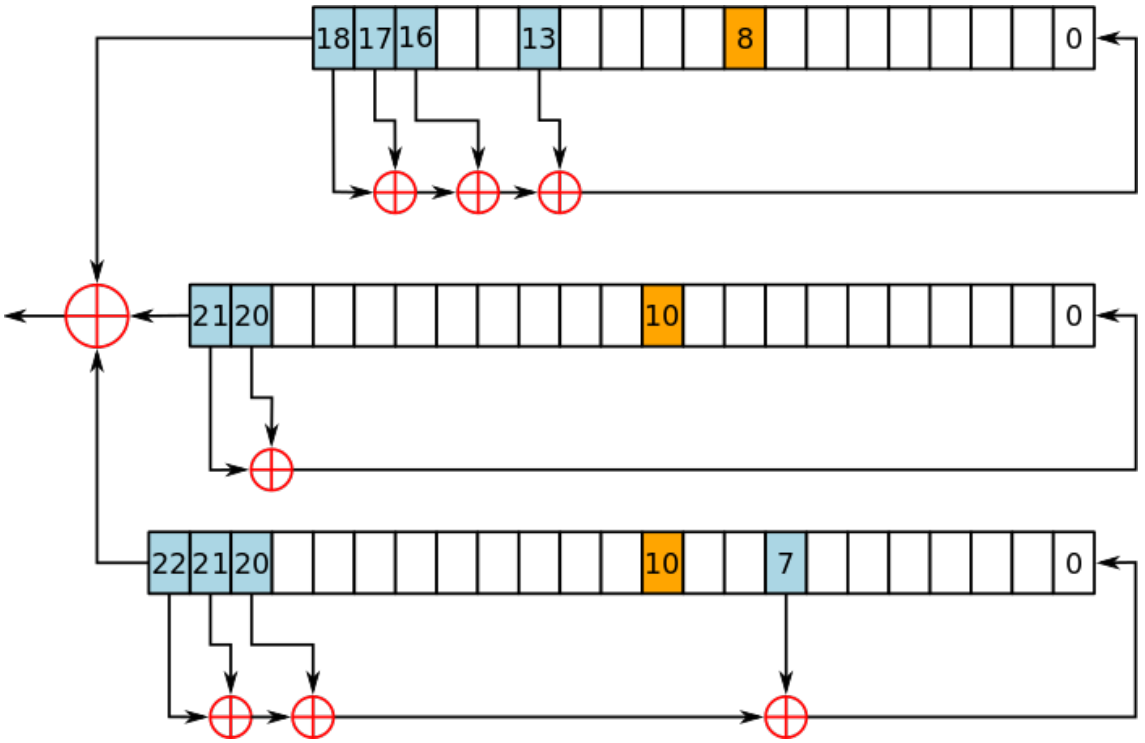
Maximal Shift Register Sequences

Shift registers do polynomial arithmetic. Maximal period shift registers, correspond to polynomials with maximal period: primitive polynomials.

Cost of Key Production

Many shift register systems were keyed with primitive polynomials. These were hard to find and key production was expensive.

GSM A5



Post World War II

Symmetric Cryptography

Stream ciphers gradually give way to block ciphers.

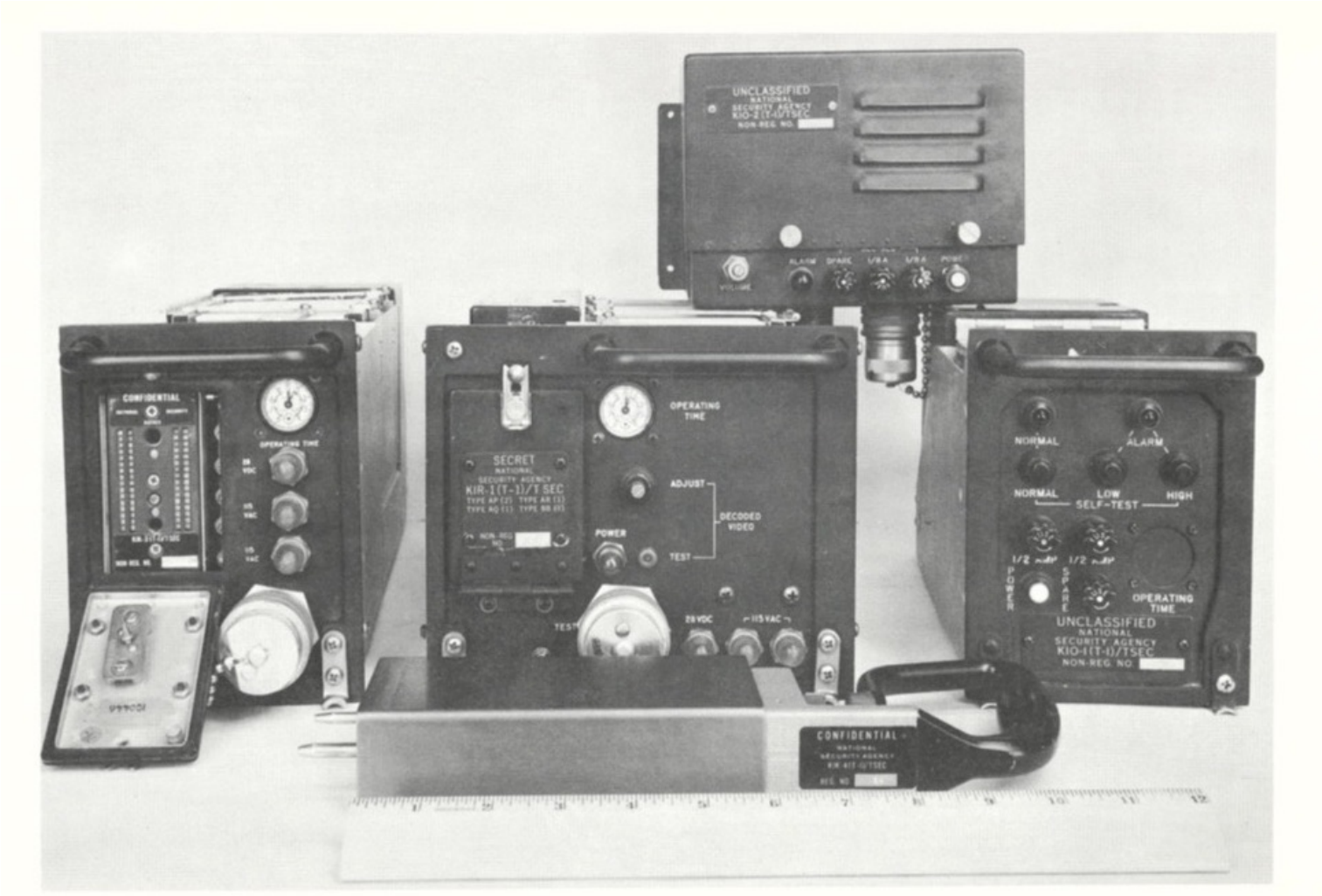
Identification Friend or Foe

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

Horst Feistel

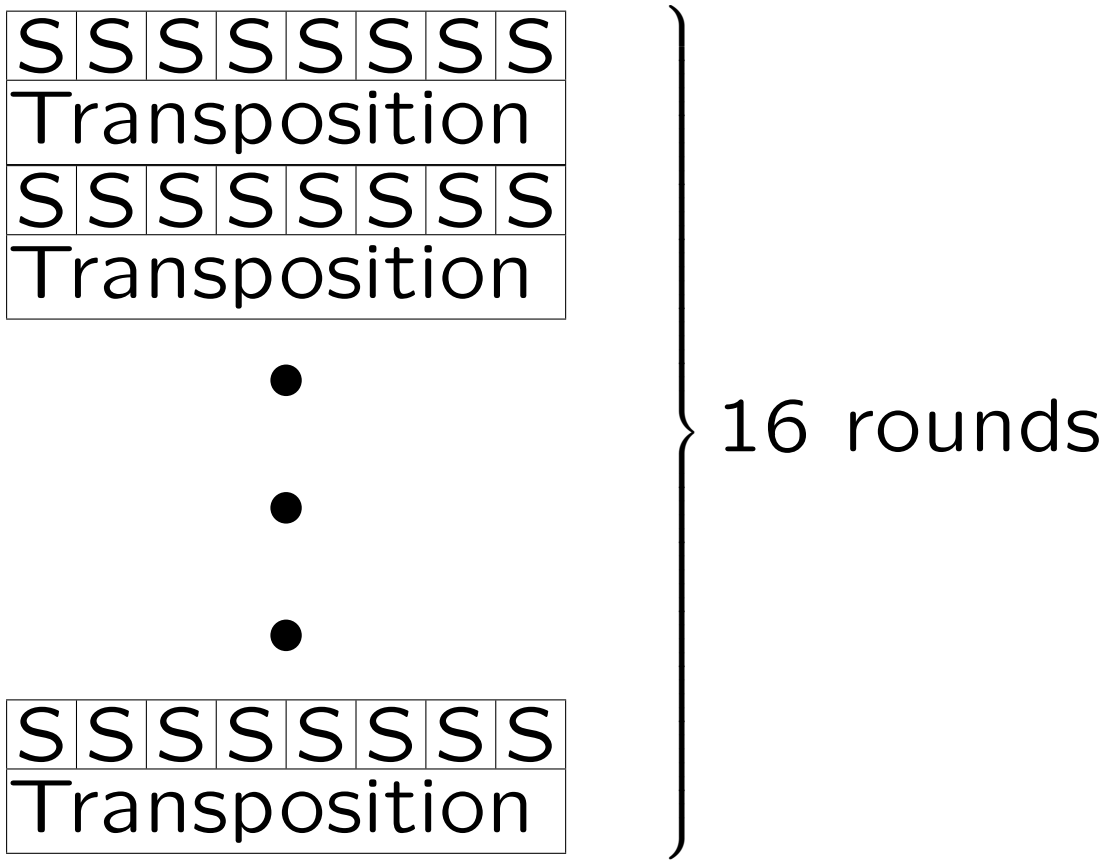
IBM 2984 Banking System

- 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

Scientific American Lucifer



Scientific American Lucifer

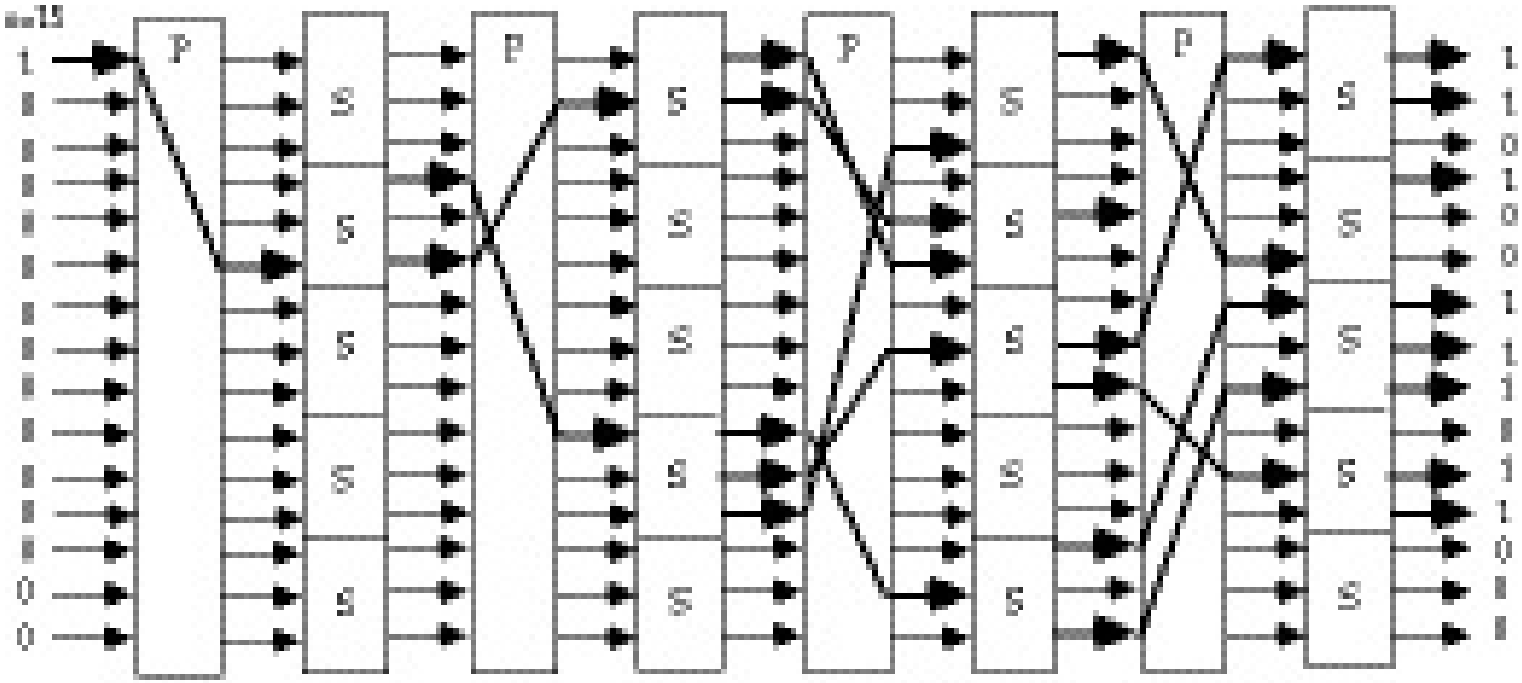


Fig 2.3 - Substitution-Permutation Network with the Avalanche Characteristic

Smith's Lucifer

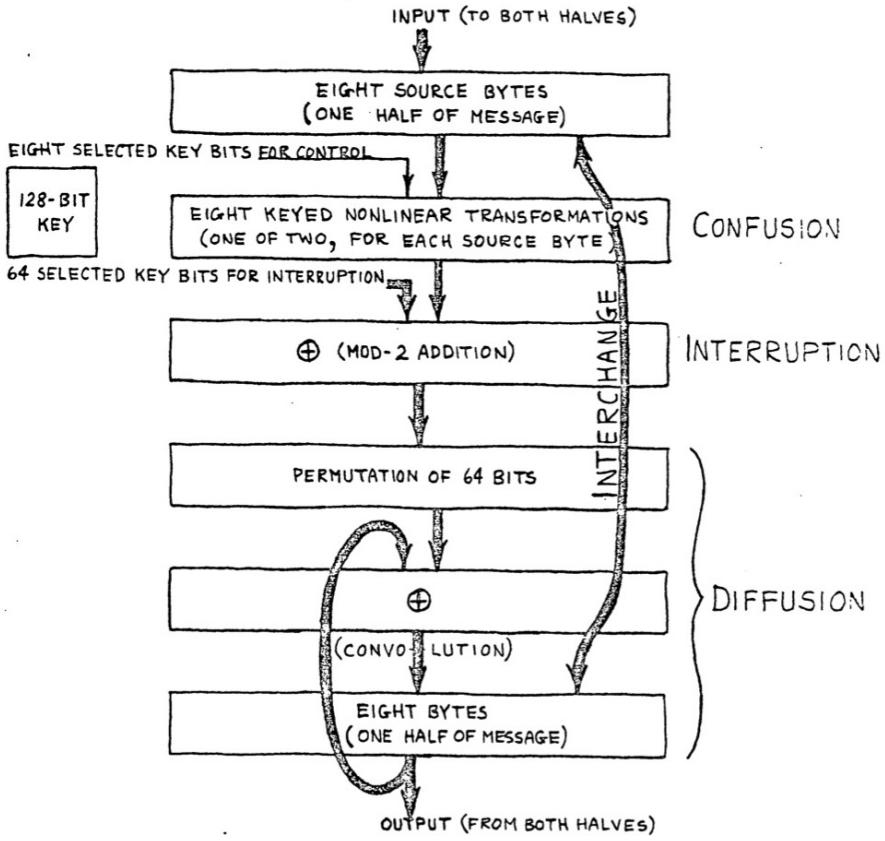
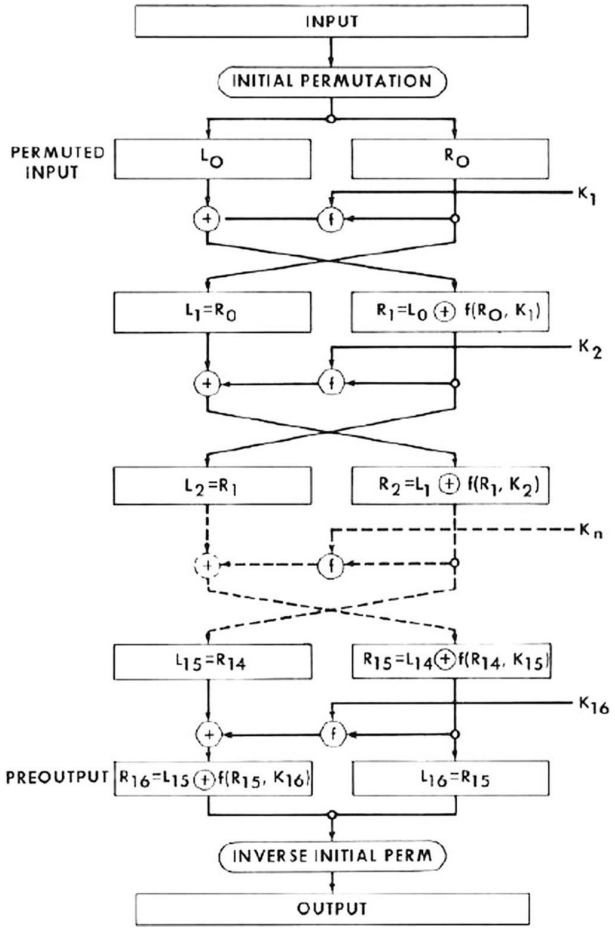


FIG. 1. FUNCTIONAL BLOCK DIAGRAM OF THE CIPHER SYSTEM

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.

Nineties and On

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

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

Key Management

Management view of Cryptography

- Crypto is an amplifier
- Separates security from path of message

Key management systems both reflect and shape the organizations that employ them.

Function of Key Management

Couples to bureaucracy: clearances, jobs ...

Elements of Key Management

- Production
  - Testing
- Shipping and Storage
- Use (to encrypt or decrypt)

Elements of Key Management? (Cont'd)

- Accounting
- Destruction

Key Production

- There is no more critical crypto function

  – If you can produce good key, you have the possibility of good cryptoography.

  – If you can't, you don't.

Generating Unpredictability (Randomness)

- Card shuffling
- Rotors
- Slot machines
- Thermal noise
- Astable multivibrators

Randomness (Cont'd)

- Atmospheric turbulence in Winchester disks
- Half-silvered mirror (ETH)
- Human variability

Desiderata

- Never seen by human eyses
  - Impossible with code books and rotors
- Failing that, secrecy of key, until traffic declassified.

Desiderata (Cont'd)

- Easy to use
- Hard to copy
- Easy to destroy

Quality Control

- Cycle reandom generator and test

- Testing for the failure of the generator, not for the quality of the method.

  – Don't hash before testing.

Key Production Costs

- Physical
  - manufacturing rotors
  - permutor boards

Key Production Costs

- Logical
  - permutations for rotor wirings
  - primitive polynomials for shift registers
  - prime numbers for RSA keys

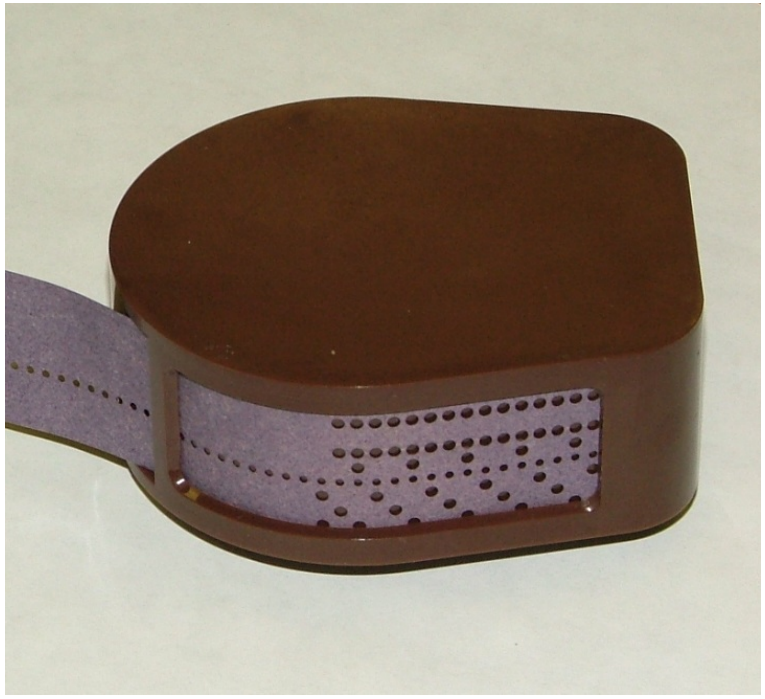
Distribution

- Shipping
- Encrypted transmission
- Quantum Key Distribution

Transport

- Paper tape in canisters
- KYK-13
- KSD64a (STU-III)
- Smart cards
- All ordinary data storage devices: CDCs, USBs, etc.

Key-tape Canister



KYK-13

KY-57


KY - 57
"VINSON"
Manpack Secure Voice
Half Duplex Wideband
Equipment shown here with PR -77 Radio
1970s - Present
TD
ON
OFF
VOLUME
AUDIO
FILL
MODE

Cable

Use

- Codebooks
- Rotor machine setup
- Plug boards
- Slide switches
- Pull paper tape, etc.

Paper-tape Key Loader

Accounting
(Comsec Materials Control System)

- Central Facility
- Comsec accounts
- Comsec Custodians and user agents
- Hand receipts
- Inventories

Destruction

- Lead jackets to sink codebooks
- Smashing rotors
- Burning or shredding cards and tapes

Destruction

- Zeroizing many forms of computer memory
- Physically destroying computer memory

Changing Keys

- Why change keys
  - Cryptoperiod (intrinsic)
  - Management issues (extrinsic)

Changing Keys

- Rekeying
- Key Updating

  – backtrack security

- Daisy chaining (danger of cascading compromise)