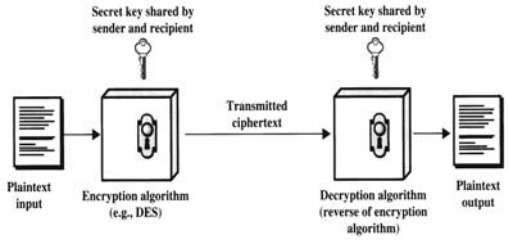
Wat is encryptie?

- Encryptie of codering
  plaintext (platte tekst) ➔ ciphertext (gecodeerd)
- Decryptie of decodering
  ciphertext ➔ plaintext
- algoritme + sleutel



enigma - SDES - DES 1

Soorten encryptie

- Conventionele encryptie
  - zender en ontvanger gebruiken dezelfde sleutel
  - synoniemen:
    geheime sleutel cryptografie
    symmetrische codering
    private sleutel cryptografie
- Publieke sleutel encryptie
  - zender en ontvanger gebruiken verschillende sleutel
  - één van de sleutels is publiek, de andere is geheim
  - synoniemen:
    asymmetrische codering
    dubbele sleutel encryptie

enigma - SDES - DES 2

Enigma

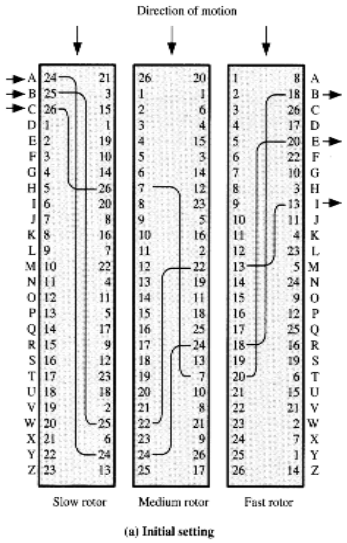
- enigma = raadsel, mysterie
- elektromechanisch rotorsysteem
- WOII (Duistland, Japan)
- ontwikkeling van computers

Enigma (2)

- dateert van begin 20ste eeuw
- samengesteld uit
  - druktoets voor elke letter
  - lichtje voor elke letter
  - stel verdraaibare schijven = rotors (3, later 4)
- rotor bevat 26 input- en 26 output-pinnen
- pinnen intern in rotor verbonden
- verbinding in elke rotor anders
- buitencontacten verbonden met toets, lamp en batterij

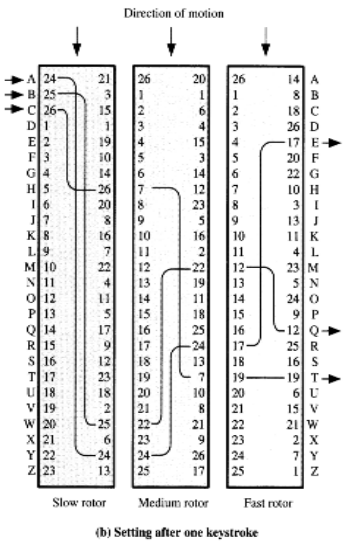
Enigma (3)

A→B



(a) Initial setting

A→E



(b) Setting after one keystroke

5

Enigma (4)

- sleutel = beginpositie rotors
- toetsaanslag ➔ rotor1 draait +1
- rotor1 volledig rondgedraaid ➔ rotor2 draait +1
- rotor2 volledig rondgedraaid ➔ rotor3 draait +1
- toetsaanslag ➔ oplichtende letter noteren
- spatie = z
- getallen voluit

- ULTRA – poject
- Coventry 14/11/1940
- 1% gebroken berichten

enigma - SDES - DES 6

ROT13

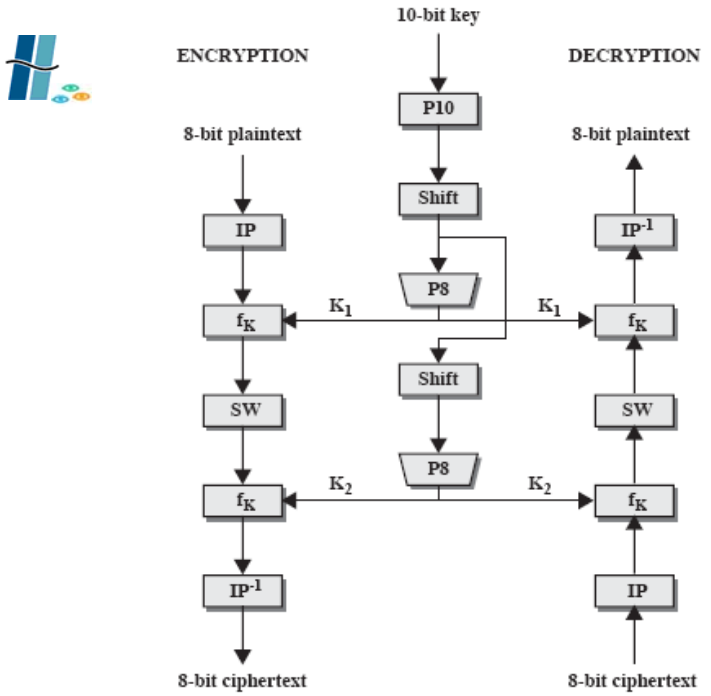
- vaste substitutie als codering
- variatie op Caesar's cipher (ROT3)
- elke letter vervangen door een andere letter die 13 plaatsen verder in alfabet staat
- `tr a-zA-Z n-za-mN-ZA-M <inputfile >outputfile`
- `Het regent weer vandaag`
  wordt
  `Urg ertrag jrre inaqnnt`
- veilig?

enigma - SDES - DES 7

SDES

- Simplified DES
- DES = Data Encryption Standard
- pedagogisch
- ontwikkeld door Edward Shaefer (University of Santa Clara)
- block cipher
- plaint text 8 bits ←→ cipher text 8 bits
- sleutel 10 bits
- gedeelde sleutel tussen zender en ontvanger

enigma - SDES - DES 8



9

SDES componenten CODEC

5 stappen (4 functies):

- initiële permutatie IP
- functie f_k
  - permutaties en substituties
  - afhankelijk van deelsleutel van 8 bits
- omwisseling SW
- f_k met tweede deelsleutel
- inverse initiële permutatie

- codering = decodering
- deelsleutels omgekeerde volgorde

enigma - SDES - DES 10

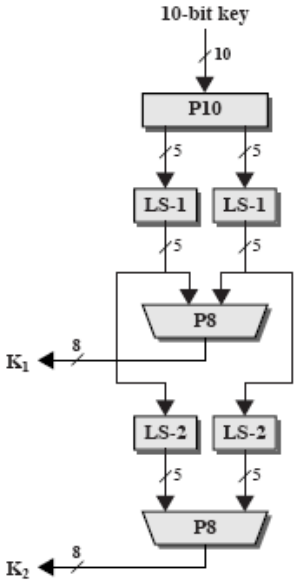
SDES sleutels

10 bit sleutel

3 functies:

- permutatie P10
- verschuiving (shift)
- permutatie P8

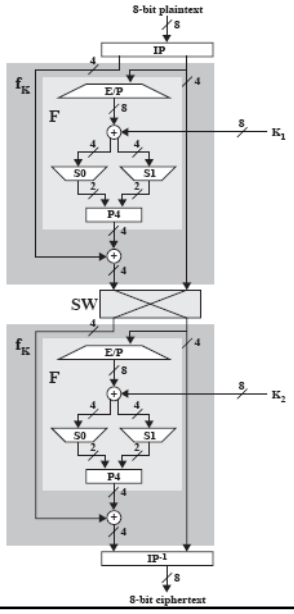
SDES sleutelgeneratie



P10:
3 5 2 7 4 10 1 9 8 6

P8:
6 3 7 4 8 5 10 9

SDES (de)codering



IP: 2 6 3 1 4 8 5 7

E/P: 4 1 2 3 2 3 4 1

S0:

1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	2

S1:

0	1	2	3
2	0	1	3
3	0	1	0
2	1	0	3

P4: 2 4 3 1

IP^{-1}: 4 1 3 5 7 2 8 6

SDES S-boxen

- S-box = matrix
- doel: bits vervangen door andere bits
- 4 invoerbits bepalen plaats:
  - bit1 bit4 → rij
  - bit2 bit3 → kolom

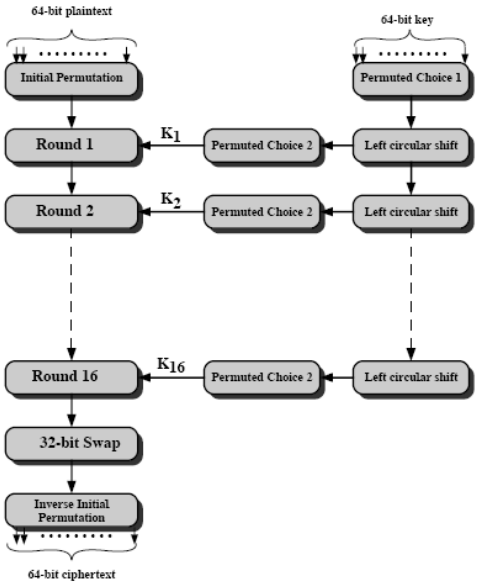
SDES sterkte

- bepaald door sleutellengte
- 10 bits ➔ 1024 verschillende sleutels
- brute force attack
- hoe correcte plain text detecteren ?

DES

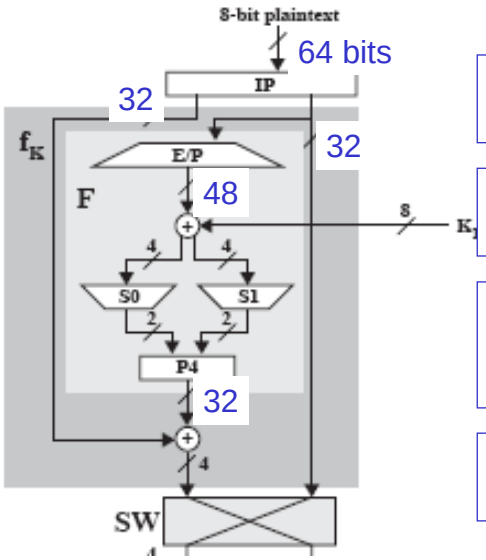
- Data Encryption Standard
- “meest” gebruikt
- ontwikkeld bij IBM in 1970
- standaard
- implementatie in devices (modems, netwerkkaarten)

DES schema



17

SDES versus DES



sleutel 56 bits ➔
16 deelsleutels 48 bits

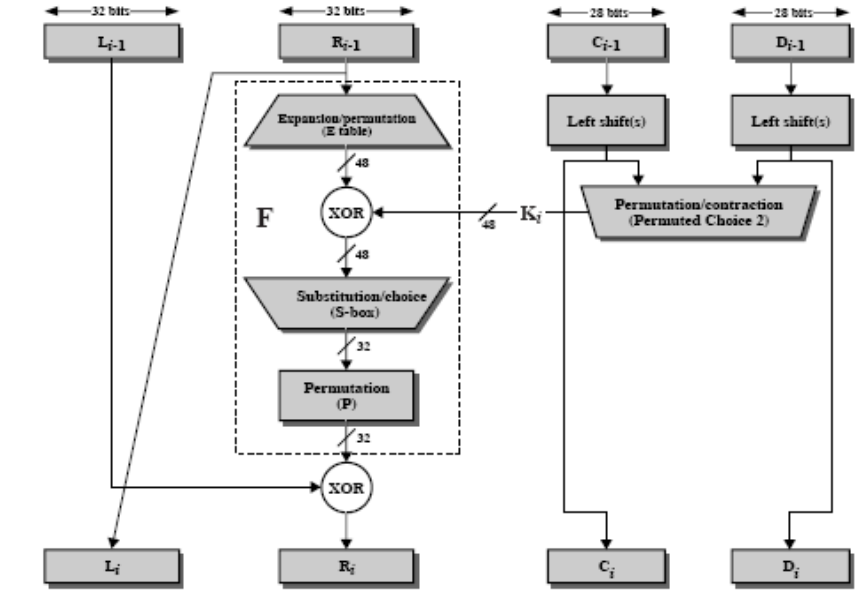
48 = 8 x 6 bits
➔ 8 S-boxen

6 bits = 2 + 4
➔ 4 rijen
➔ 16 kolommen

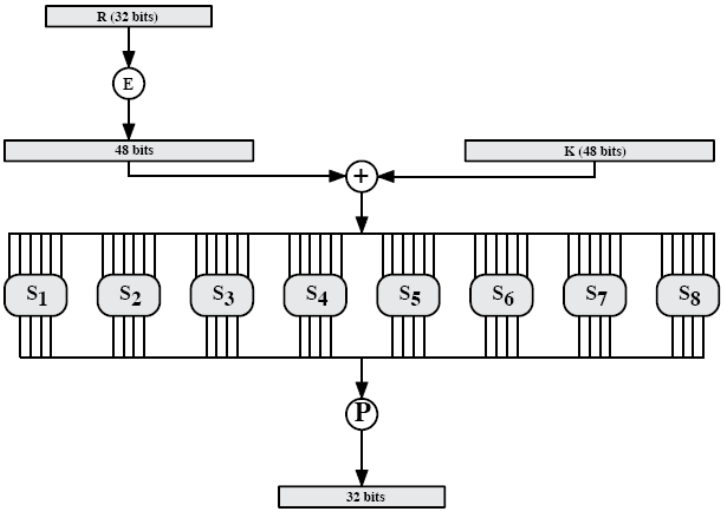
1 el van S-box: 4 bits
x8 boxen = 32 bits

18

DES ronde



DES berekening van F



enigma - SDES - DES 20

Sterkte van DES

Sleutellengte

- key 56 bits → 2^{56} = 7,2 x 10^{16} sleutels uitproberen
- stel: encryptie=1µs (??) en raak na ½ van sleutels
  1 jaar = 3,1 x 10^{13} → duur > 1000 jaar
- known plaintext attack:
  - DH (1977): plan bouw parallelle machine met bestaande technologie, 10^6 encryptiedevices, 10u, 20 M$
  - Wiener (1993): theoretische chip, cfr DH, 21 min, 10 M$
  - RSA secret key challenge (1997):
    10.000 $ beloning, "the unknown message is"
    96 dagen, gedistribueerd
  - Electronic Frontier Foundation (1998)
    DES cracker machine gebouwd voor $ 250.000, aanval < 3 dagen

Sterkte van DES (2)

- anders: hoe herken je de plaintext?
  compressie vóór encryptie
  niet-tekst info

Aard van DES- algoritme

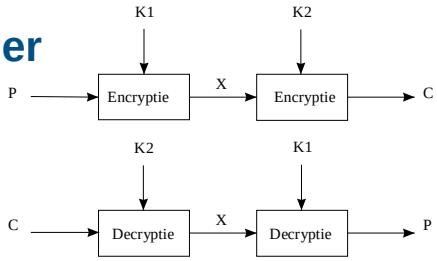
- ontwerpcriteria van S-boxen
  - niet publiek gekend
  - onregelmatig gedrag van S-Boxen nog niet gebruikt in aanval

Timing attacks

- gebaseerd op licht verschil in tijd tssn COD en DEC
- DES tamelijk resistent
- sneeuwbaleffect (1bit wijzigen → 34 na 16 ronden)

DES veiliger

Double DES



meet in the middle attack (known plaintext)

$C = E_{K2}[X]$

$X = E_{K1}[P] = D_{K2}[C]$

voor elk paar [P,C]
- bereken alle E[P] en D[C]
- bepaal overeenkomst

DES veiliger (2): Triple DES