

Vraag 1)

a. 2x Caesar

JAHHKRUV

DUBBELOP

b.

EEASNENIDNSTATPINROE

{'E': 4, 'N': 4, 'A': 2, 'S': 2, 'I': 2, 'T': 2, 'D': 1, 'P': 1, 'R': 1, 'O': 1}

EEASNENIDN

STATPINROE

EESI

ENTN

AIAR

SDTO

NNPE

EEASN

ENIDN

STATP

INROE

EEAS

NENI

DNST

ATPI

NROE

(ENDANEENTRANSPOSITIE)

c. Een affine cipher

Vraag 2)

a. $20 * 1/(20^2) = 1/20$ ($\text{len}(\text{ABCDEFGHIJKLMNOPQRSTUVWXYZ}) = 20$)

b. 0.066

c. Een onbekende periode kan geschat worden op basis van de IoC als volgt:

$p \approx (\text{Engelse IOC} - \text{Random IOC} / \text{Gevonden IOC} - \text{Random IOC}) = 0.028 / (0.042 - 0.038) \approx 7$

- d. ϕ -test
- e. Een transpositie is een permutatie van de posities en een substitutie een per-mutatie van de objecten.

Vraag 3)

a.

- i. $(25, 22) = ZW$
- ii. $HI = (8, 9)$
 $(8, 9) - (1, 1) = (7, 8)$
 $In\ modern = (6, 7)$
 Originele matrix:
 $\begin{bmatrix} 0 & 3 \\ 3 & 0 \end{bmatrix}$
 Determinant: $0 - 9 = -9 = 17 \pmod{26}$

Inverse matrix:

$$\frac{1}{\det(M)} * \begin{bmatrix} a & -b \\ -c & d \end{bmatrix}$$

inverse van determinant is dus modulair inverse (17 invers =

23)

$$23 * \begin{bmatrix} 0 & -3 \\ -3 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 9 \\ 9 & 0 \end{bmatrix}$$

// Legacy -> Modern -> Legacy

$$\begin{bmatrix} 0 & 9 \\ 9 & 0 \end{bmatrix} * ([6]) = \begin{bmatrix} 0 & 9 \\ 9 & 0 \end{bmatrix} * [6] = \begin{bmatrix} 11 \\ 1 \end{bmatrix} + [1] = \begin{bmatrix} 12 \\ 2 \end{bmatrix} = L$$

$$\begin{bmatrix} 0 & 9 \\ 9 & 0 \end{bmatrix} * ([7]) = \begin{bmatrix} 0 & 9 \\ 9 & 0 \end{bmatrix} * [7] = \begin{bmatrix} 2 \\ 3 \end{bmatrix} + [1] = \begin{bmatrix} 3 \\ 4 \end{bmatrix} = C$$

// Legacy

$$\begin{bmatrix} 0 & 9 \\ 9 & 0 \end{bmatrix} * ([7]) = \begin{bmatrix} 0 & 9 \\ 9 & 0 \end{bmatrix} * [7] = \begin{bmatrix} 20 \\ 7 \end{bmatrix} = T$$

$$\begin{bmatrix} 0 & 9 \\ 9 & 0 \end{bmatrix} * ([8]) = \begin{bmatrix} 0 & 9 \\ 9 & 0 \end{bmatrix} * [8] = \begin{bmatrix} 11 \\ 8 \end{bmatrix} = K$$

b.

- i. De substitutie bestaat uit een vermenigvuldiging met 3 gevolgd door een optelling met 1
- ii. De transpositie is een verwisseling van twee karakters per paar

Vraag 4)

a. ALEPH1
BCDFGI
JKMNOQ
RSTUVW
XYZ023
456789

F = DG
A = AA
A = AA
A = AA
F = DF
H = AV
F = DG
I = DX

b. STRAND

DGAAAA
AADFAV
DGDY

ADNRST

A

F

X

etc

AGADAAVDDGAADXFA

P L A Y F A I R

vraag 5)

a. IHEKV

b. (AB)(ST)(QR)(OP)(OP)

ATROP (porta omgedraaid)

Hele tekst: HIERINISPORTAVERBORGEN

vraag 6)

DMAIEWGEALJZIKWALNTJWELE

vraag 7)

a $E(a) = a^e \bmod p$

b

a	1	2	3	4	5	6	7	8	9	10	11
E(a)	1	8	4	18	10	9	21	6	16	11	20

c

d

$$d = e^{-1} \bmod p - 1$$

$$= 3^{-1} \bmod 22$$

$$d = 15$$

vraag 8)

a

Een klaartekstblok in DES bestaat uit **64** bits.

| ABCDEFGHI JKLM

---+-----

AB | NOPQRSTUVWXYZ

CD | OPQRSTUVWXYZN

EF | PQRSTUVWXYZNO

GH | RQRSTUVWXYZNOP

IJ | RSTUVWXYZNOPQ

KL | STUVWXYZNOPQR

MN | TUVWXYZNOPQRS

OP | UVWXYZNOPQRST

QR | VWXYZNOPQRSTU

ST | WXYZNOPQRSTUV

UV | XYZNOPQRSTUVW

WX | YZNOPQRSTUVWXYZ

YZ | ZNOPQRSTUVWXYZ

Elke S-box heeft een input van **6** bits en een output van **4** bits.

DES gebruikt een **Feistelnetwerk** met **16** rondes.

Triple DES heeft een sleutellengte van **56 * 3 = 168** bits.

AES-lagen:

S-Boxes / SubBytes

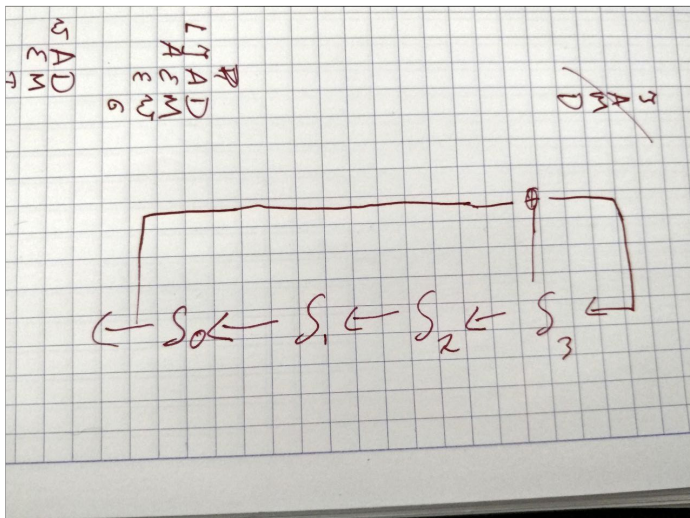
Rotations / ShiftRows

Hill cipher / MixColumns

Add round key / AddKey

vraag 9)

a



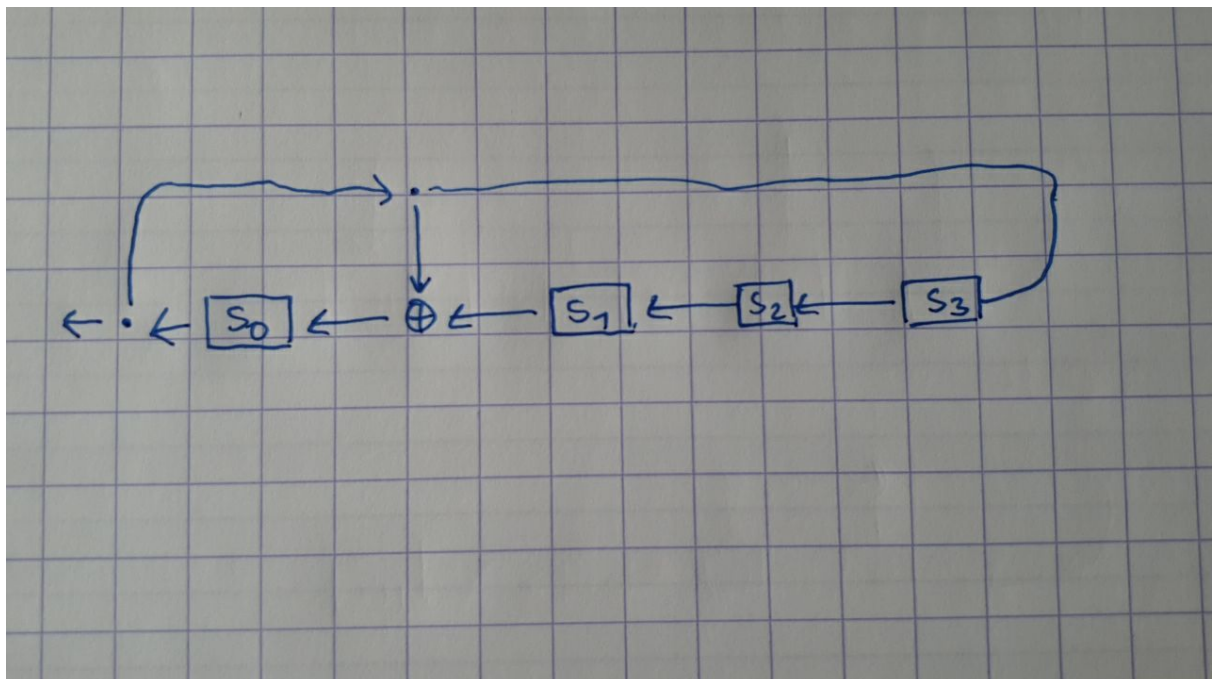
b

$$F(s) = s_0 \text{ XOR } s_3$$

0001
0011
0111
1111
1110
1101
1010
0101
1011
0110
1100
1001
0010
0100
1000
0001

000111101011001

c



vraag 10)

a

$$\begin{aligned}\varphi(18) &= \varphi(2) * \varphi(3^2) \\ &= (2 - 1)(3*2) \\ &= 6\end{aligned}$$

b

In Z_{18}^* missen de veelvouden van 2 en 9, aangezien dat de priemgetalfactorizatie is van 18.

.	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7		13	5	1	11
11	11			13	17	7
13	13				7	5
17	17					1

c Ja, 5 en 11 zijn generatoren.

13, $13 \cdot 13 = 7$, $13 \cdot 7 = 1$, $13 \cdot 1 = 13$ X

5, $5 \cdot 5 = 7$, $7 \cdot 5 = 17$, $17 \cdot 5 = 13$, $13 \cdot 5 = 11$, $11 \cdot 5 = 1$

7, $7 \cdot 7 = 13$, $13 \cdot 7 = 1$, $1 \cdot 7 = 7$

11, $11 \cdot 11 = 13$, $13 \cdot 11 = 17$, $17 \cdot 11 = 7$, $7 \cdot 11 = 5$, $5 \cdot 11 = 1$

d

$aX^4 + bX^3 + cX^2 + dX + e$

Spaanse monoalfabeet

ADHRF SID QINVJX IH XDNAJIXJHAD VFH YINEVJ
TENGO QUE BUSCAR UN RESTAURANTE CON MUSICA

YDZEVJHJ PFO J TTDPJX J YE PDVEHJ JTTE
MEXICANA VOY A LLEVAR A MI VECINA ALLI

DNAJ HFVWD DTTJ DN YIO QFHEAJ O NEYLJAEVJ
ESTA NOCHE ELLA ES MUY BONITA Y SIMPATICA

DNLDXF WJVDX IHJ EYLDNEFH QIDHJ
ESPERO HACER UNA IMPRESION BUENA

ABCDEFGHIJKLMNOPQRSTUVWXYZ
T EIO NUA P SYVBGQ LCH MX

Porta met crib

COLLISION

121112122

212221211

 INQ UIRYW ILLCO
MPHSY XBLAM IZXJK GXKJD WNRQM
12122 21111 12211 12111 22221
 EIM CEOEM CEMC
 FJN DFPFN DFND

 EN SEPTE MBERT
MGSIR GAKFH MYGVH ETIEX NQXDE
11212 11111 12121 12112 22211
 EIM CEOEM CEMC
 FJN DFPFN DFND

 HE COLLI SIONB
AXMDR KGRXU AYEYX QMSNO EXIMQ
12112 11222 12122 21222 12112
 EIM CEOEM CEMC
 FJN DFPFN DFND
 IN DEPENDENCE

 LA STSAT URDAY
SEIWR FGWJR XKDPT EELPA GCWOJ
21122 11212 21122 11121 11221
 EIM CEOEM CEMC

FJN DFPFN DFND