

Naam: _____

Studentnummer: _____

Aanwijzingen voor dit tentamen

- Schrijf je naam en studentnummer op elk in te leveren vel, inclusief de tentamenvellen.
- Lees de vragen zorgvuldig en besteed niet te veel tijd aan één enkele opgave.
- Schrijf duidelijk met blauwe of zwarte pen en gebruik géén potlood.
- Er is ruimte voor de antwoorden op het tentamenvel.
- Gebruik alleen indien nodig het extra tentamenpapier.
- Bij meerkeuzevragen is één antwoord juist.
- Succes met dit tentamen!

Vraag 1: Eenvoudige systemen..... (totaal 10 punten)

(4 punten) (a) In deze opgave is een eenvoudige sleutelloze vercijfering twee keer achter elkaar toegepast.

Ontcijfer JAHHKRUV.

(a) _____

(4 punten) (b) Nu wat anders.

Ontcijfer EEASNENIDNSTATPINROE.

(b) _____

(2 punten) (c) Hoe noemen we de samenstelling van een decimatie met een additieve vercijfering?

(c) _____

Vraag 2: Theorie..... (totaal 10 punten)

(2 punten) (a) Wat is de verwachte Index of Coincidence van een random tekst bij gebruik van alleen de letters ABCDEFGHIJKLMNOPQRST?

(a) _____

(2 punten) (b) Wat is de verwachte Index of Coincidence voor een normale Engelse tekst?

(b) _____

(2 punten) (c) Een met een sleutelwoord polyalfabetisch versleutelde tekst heeft een Index of Coincidence van 0.042.

Wat is een goede aanname voor de lengte van het sleutelwoord?

(c) _____

- (2 punten) (d) Welke test gebruikt de Index of Coincidence voor de bepaling van de monoalfabeticiteit van een gegeven tekst?
- ☐ Chi(χ)-test
 - ☐ Kappa(κ)-test
 - ☐ Phi(ϕ)-test
 - ☐ Geen van de drie vorige items
- (2 punten) (e) Als we een tekst opvatten als een afbeelding van een verzameling posities naar een verzameling objecten (symbolen), dan geldt:
- ☐ Een substitutie en een transpositie zijn beide permutaties van de objecten.
 - ☐ Een substitutie en een transpositie zijn beide permutaties van de posities.
 - ☐ Een substitutie is een permutatie van de posities en een transpositie een permutatie van de objecten.
 - ☐ Een transpositie is een permutatie van de posities en een substitutie een permutatie van de objecten.
 - ☐ Geen van de vier vorige items is juist.

Vraag 3: **Hillvercijfering** (totaal 10 punten)

- (a) Laat een affiene Hillvercijfering gegeven zijn door

$$\begin{pmatrix} 0 & 3 \\ 3 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} \pmod{26}$$

- (3 punten) i. Wat is de vercijfering van HI in **moderne** encoding?

i. _____

- (3 punten) ii. Wat is de **ont**cijfering van HI in **legacy** encoding?

ii. _____

- (b) Beschrijf deze Hillvercijfering als de samenstelling van

- (2 punten) i. een substitutie

i. _____

- (2 punten) ii. en een transpositie

ii. _____

Naam:

Studentnummer:

Vraag 4: **ADFGVX** (totaal 10 punten)

We beschouwen de ADFGVX-vercijfering,
gebaseerd op het alfabet ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789.

- (4 punten) (a) Construeer het 6x6-sleutelvierkant, gemaakt met de sleutel ALEPH1.

	A	D	F	G	V	X
A						
D						
F						
G						
V						
X						

- (2 punten) (b) Vertaal met behulp van de tabel uit deel (a) de tekst FAAAFHFI naar een cryptogram, bestaande uit alleen letters in ADFGVX.

(b) _____

- (4 punten) (c) Ontcijfer vervolgens het gevonden cryptogram uit deel (b), met gebruikmaking van de sleutel STRAND voor de kolomtranspositie die in de ADFGVX-vercijfering gebruikt wordt.

(c) _____

Vraag 5: **Porta** (totaal 10 punten)

Je vindt een Portatabel aan het eind van het tentamen,

- (6 punten) (a) De cijfertekst URZKPARKIHEKVBYEXGKNRE is met Porta versleuteld en bevat de tekst porta als crib. Welk stuk van de cijfertekst correspondeert hiermee?

(a) _____

- (4 punten) (b) Welk sleutelwoord van vijf letters zou hier gebruikt kunnen zijn?

(b) _____

Vraag 6: **Routetranspositie** (totaal 8 punten)

- (8 punten) (a) Los de routetranspositie DMAIEWGEALJZIKWALNTJWELE op.

(a) _____

Naam:

Studentnummer:

Vraag 7: **Pohlig-Hellmanencryptie**..... (totaal 10 punten)

We werken modulo het priemgetal $p = 23$. Als exponent voor encryptie kiezen we $e = 3$.

(2 punten) (a) Wat is de formule voor Pohlig-Hellmanencryptie?

(a) _____

(4 punten) (b) Vul de encryptietabel in:

a	1	2	3	4	5	6	7	8	9	10	11
$\mathcal{E}(a)$											

(2 punten) (c) Hoe kun je snel met behulp van de tabel uit deel (b) aflezen wat $\mathcal{E}(17)$ is?

(c) _____

(2 punten) (d) Bereken de exponent d die de bijbehorende decryptie oplevert.

(d) _____

Vraag 8: **Blokcijfers**..... (totaal 10 punten)

(a) We beschouwen DES.

- (1 punt) i. Een klaartekstblok in DES bestaat uit _____ bits.
- (2 punten) ii. Elke S-box heeft een input van _____ bits en een output van _____ bits.
- (2 punten) iii. DES gebruikt een _____ netwerk met _____ rondes.
- (1 punt) iv. Triple DES heeft een sleutellengte van _____ bits.

(b) We beschouwen AES.

Benoem de vier lagen van AES.

(1 punt) _____

(1 punt) _____

(1 punt) _____

(1 punt) _____

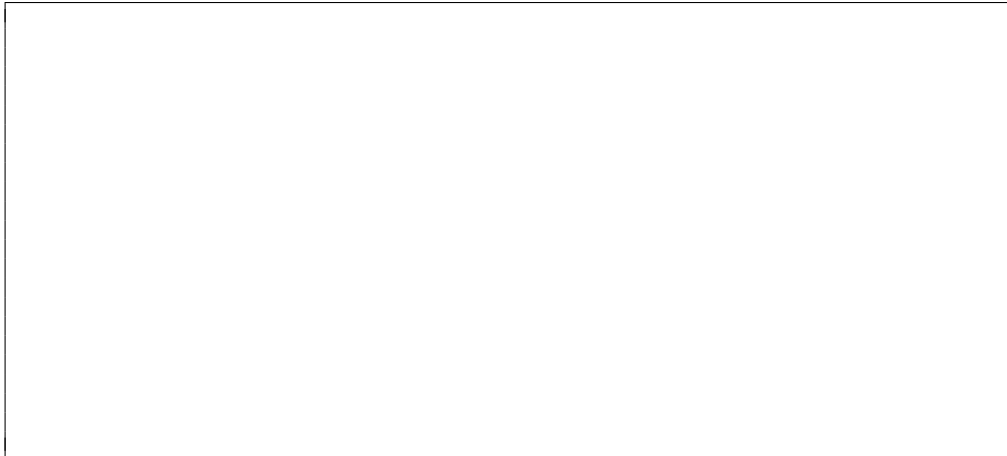
Naam:

Studentnummer:

Vraag 9: **Schuifregisters** (totaal 10 punten)

We beschouwen een lineair teruggekoppeld Fibonacci-schuifregister met als terugkoppelpolynoom $X^4 + X + 1$.

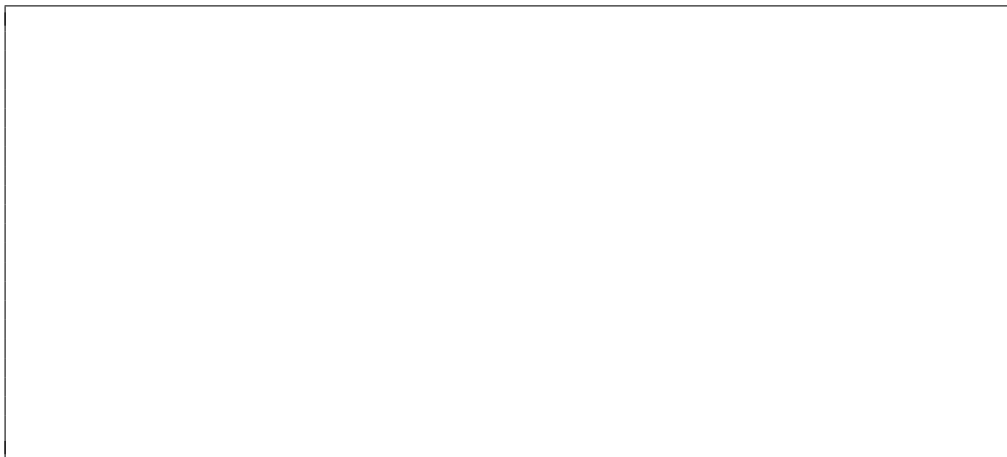
- (3 punten) (a) Maak een tekening van dit Fibonacci-schuifregister met de taps op de juiste plaats.



- (4 punten) (b) Maak de sleutelstroom af die begint met 0001. Stop na één volledige periode.

(b) _____

- (3 punten) (c) Maak een tekening van het gerelateerde Galois-schuifregister dat dezelfde sleutelstroom genereert.



Naam:

Studentnummer:

Vraag 10: **Getaltheorie**.....(totaal 12 punten)

We beschouwen $\mathbb{Z}_{18}^*$, de groep van inverteerbare restklassen modulo 18.

(2 punten)

(a) Bereken $\phi(18)$

(a) _____

(4 punten)

(b) Vul het bij $\mathbb{Z}_{18}^*$ horende vermenigvuldigingschema in.
Laat ongebruikte kolommen en rijen leeg.

.								

(3 punten)

(c) Is $\mathbb{Z}_{18}^*$ cyclisch?
Zo ja, wat zijn de generatoren?
Zo nee, waarom niet?

(c) _____

(3 punten)

(d) Welk polynoom van graad 4 over $\mathbb{Z}_2$ is reducibel, maar heeft geen nulpunt?

(d) _____

Naam:

Studentnummer:

Portatabel:

```
| ABCDEFGHI JKLM
---+-----
AB|NOPQRSTUVWXYZ
CD|OPQRSTUVWXYZN
EF|PQRSTUVWXYZNO
GH|QRSTUVWXYZNOP
IJ|RSTUVWXYZNOPQ
KL|STUVWXYZNOPQR
MN|TUVWXYZNOPQRS
OP|UVWXYZNOPQRST
QR|VWXYZNOPQRSTU
ST|WXYZNOPQRSTUV
UV|XYZNOPQRSTUVW
WX|YZNOPQRSTUVWX
YZ|ZNOPQRSTUVWXY
```

Vraag	Punten	Score
Eenvoudige systemen	10	
Theorie	10	
Hillvercijfering	10	
ADFGVX	10	
Porta	10	
Routetranspositie	8	
Pohlig-Hellmanencryptie	10	
Blokcijfers	10	
Schuifregisters	10	
Getaltheorie	12	
Totaal	100	