GEBRUIK VAN **ENDECRYPT**, **MATHEMATICA** EN **MATLAB** WORD TOEGELAAT

Universiteit van Stellenbosch
Toegepaste Wiskunde 314
Semestertoets II
14 Junie 2003
Tyd: 09:00-12:00 Punte: 100

Vul asseblief in / *Please complete*:

Van (blokletters) / *Surname (capitals)*
Volle Voorname / *Full First Names*
US–nommer / *US Number*

Vir kantoorgebruik / *For official use*

Vraag *Question*	Punte *Marks*	Nasiener *Marker*
1	/17	J. van Vuuren
2	/13	J. van Vuuren
3	/16	P. Grobler
4	/16	P. Grobler
5	/19	P. Grobler
6	/19	P. Grobler
Totaal	/100	

Eksaminatore / Examiners: J.H. van Vuuren & P.J.P. Grobler

Lees asseblief die volgende reëls en voorskrifte, en teken dan die onderstaande verklaring:

(1) Kommunikasie tussen kandidate word nie in die eksamenlokaal toegelaat nie.

(2) Hulpmiddels (insluitende blankopapier, boeke, geskrifte en elektroniese apparaat) word nie in die eksamenlokaal toegelaat nie, tensy die gebruik van spesifieke items uitdruklik toegelaat of voorgeskryf is.

(3) Geen dele van hierdie vraestel/antwoordstel mag verwyder word nie.

(4) Ekstra tyd word nie toegestaan aan kandidate wat laat kom nie.

(5) Kandidate word nie toegelaat om die eksamenlokaal binne die eerste 45 minute van die eksamensessie te verlaat nie.

(6) Antwoorde mag in potlood ingevul word.

(7) Hierdie vraestel sowel as u antwoordstel moet aan 'n opsiener oorhandig word voordat u die eksamenlokaal verlaat.

Please read the following rules and instructions, and then sign the declaration below:

(1) Communication between candidates is not allowed.

(2) Supporting material (including blank paper, books, notes and electronic equipment) is not allowed in the examination room, unless the use of particular items is expressly allowed or prescribed.

(3) No parts of this question/answer paper may be removed.

(4) Latecomers are not allowed extra time.

(5) Candidates are not allowed to leave the examination room within the first 45 minutes of the examination session.

(6) Answers may be supplied in pencil.

(7) Before leaving the examination room candidates must hand this question paper as well as solutions to an invigilator.

VERKLARING / *DECLARATION*	HANDTEKENING / *SIGNATURE*
Hiermee verklaar ek dat ek die bogenoemde eksamenreëls sal gehoorsaam en dat die inligting op hierdie bladsy verstrek, korrek is. / *I hereby declare that I will abide by the above examination rules and that the particulars supplied on this front cover are correct.*	

(1) (a) Definieer wat bedoel word met 'n *primitiewe* polinoom in $(\mathbb{Z}_2, +, \times)$. / *Define what is mean by a* primitive *polynomial in* $(\mathbb{Z}_2, +, \times)$. [2]

(b) Gebruik **Mathematica** om te toets of die volgende polinome primitief is, of nie. Motiveer volledig. / *Use* **Mathematica** *to determine whether the following polynomials are primitive, or not. Motivate fully* [5]

i. $f_1(x) = 1 + x^2 + x^6$,

ii. $f_2(x) = 1 + x^3 + x^6$,

iii. $f_3(x) = 1 + x^5 + x^6$.

(c) Waarom is primitiewe polinome belangrik by die studie van stroomsyfer stelsels? / *Why are primitive polynomials important in the study of stream ciphers?* [2]

(d) Gebruik 'n *Vernam stroomsyfer stelsel* waarvan die sleutelstroom gegenereer word deur die lineêre terugvoer–skuifregister $\mathcal{F}^5_{1+x^5+x^6}$ met begintoestand $[1, 1, 0, 0, 0, 1]$ om die kriptoteks `11000001 00010001` te dekripteer. Wat is die ooreenstemmende skoonteks (i.t.v. Romeinse karakters)? Wys u werking. / Use a *Vernam stream cipher* whose key stream is generated by the linear feedback shift register $\mathcal{F}^5_{1+x^5+x^6}$ with initial state $[1, 1, 0, 0, 0, 1]$ to decrypt the ciphertext `11000001 00010001`. What is the corresponding plaintext (i.t.o. Roman characters)? Show your working. [3]

(e) Die binêre stroom $\underline{s} = 1,1,0,0,1,1,0,1,1,1,1,1\ldots$ is deur middel van 'n lineêre terugvoer–skuifregister, $\mathcal{F}^6_{f_4(x)}$, gevorm. Gebruik tegnieke uit *lineêre algebra* om die terugvoer–polinoom $f_4(x)$ te bepaal. / *The binary stream* $\underline{s} = 1,1,0,0,1,1,0,1,1,1,1,1\ldots$ *was formed by means of a linear feedback shift register,* $\mathcal{F}^6_{f_4(x)}$. *Use techniques from linear algebra to determine the feedback polynomial,* $f_4(x)$. [5]

(2) (a) Gebruik *Fermat se Klein Stelling* as uitgangspunt en bewys dat die orde van $\alpha \in \mathbb{Z}_n^*$ in die groep $(\mathbb{Z}_n^*, \times)$ 'n deler van $n-1$ is, indien n priem is. / *Use* Fermat's Little Theorem *as a point of departure, and prove that the order of* $\alpha \in \mathbb{Z}_n^*$ *in the group* $(\mathbb{Z}_n^*, \times)$ *is a divisor of* $n-1$*, if* n *is prime.* [3]

(b) Wat is die *orde* van $\alpha = 13$ in die groep $(\mathbb{Z}_{41}^*, \times)$? / *What is the* order *of* $\alpha = 13$ *in the group* $(\mathbb{Z}_{41}^*, \times)$*?* [1]

(c) Gebruik *Shanks se Algoritme* om die diskrete logaritme $\log_\alpha \beta \pmod{n}$ te bereken, waar $\alpha = 13$, $\beta = 11$ en $n = 41$. Produseer beide die lyste $(i, \beta\alpha^{-i} \pmod{n})$ en $(j, \alpha^{mj} \pmod{n})$, vir $i, j = 0, \ldots, m-1$, waar $m = \lceil\sqrt{n-1}\rceil$, en toon hoe u die logaritme bereken. Toets die korrektheid van u oplossing deur middel van modulêre magsverheffing. / *Use* Shanks' Algorithm *to compute the discrete logarithm* $\log_\alpha \beta \pmod{n}$, *where* $\alpha = 13$, $\beta = 11$ *and* $n = 41$. *Produce both the lists* $(i, \beta\alpha^{-i} \pmod{n})$ *and* $(j, \alpha^{mj} \pmod{n})$, *for all* $i, j = 0, \ldots, m-1$, *where* $m = \lceil\sqrt{n-1}\rceil$, *and show how you determine the discrete logarithm. Test the validity of your answer via modular exponentiation.* [5]

(d) Die kriptoteks $(11, 4)$ is deur middel van die *ElGamal*–sisteem gevorm, en is vir 'n gebruiker met publieke sleutelgetalle soos in vraag 2(c) bedoel. Wat is die ooreenstemmende skoonteks (i.t.v. Romeinse karakters)? / *The ciphertext* $(11, 4)$ *was formed via the* ElGamal–*cipher, and is intended for a user with public keys as in question 2(c). What is the corresponding plaintext (i.t.o. Roman characters)?* [2]

(e) Wat is die waarde van die masker, k, wat in vraag 2(d) tydens enkripsie gebruik is? / *What is the value of the mask, k, that was used in question 2(d) during encryption?* [2]

(3) (a) Definieer 'n q–êre kode van lengte n. / *Define a q–ary code of length n.* [1]

(b) Laat d die minimum afstand van 'n kode C wees. Bewys dat, as $d \geq 2t+1$, dan kan C t foute in enige kodewoord korrigeer. / *Let d be the minimum distance of a code C. Prove that, if $d \geq 2t+1$, then C can correct t errors in any codeword.* [5]

(c) Konstrueer 'n / *Construct a*

i. binêre $(5, 2, 5)$–kode. / *binary* $(5, 2, 5)$*–code.* [1]

ii. binêre $(5, 4, 3)$–kode. / *binary* $(5, 4, 3)$*–code.* [2]

iii. ternêre $(3, 9, 2)$–kode. / *ternary* $(3, 9, 2)$*–code.* [3]

(d) Beskou die kode $C = \{00100, 00011, 11111, 11000\}$. / *Consider the code* $C = \{00100, 00011, 11111, 11000\}$.

i. Wat is die parameters van C en hoeveel foute kan C korrigeer? / *What is the parameters of C and how many errors can C correct?* [2]

ii. Dekodeer die ontvangde vektore 11100, 01110 en 00111. / *Decode the received vectors 11100, 01110 and 00111.* [2]

(4) (a) Definieer 'n q–êre lineêre kode van lengte n. / *Define a q–ary linear code of length n.* [1]

(b) Laat C 'n lineêre kode wees en laat $w(C)$ die kleinste van die gewigte van die nie-nul kodewoorde van C wees. Bewys dat $d(C) = w(C)$. / *Let C be a linear code and let $w(C)$ be the smallest of the non–zero codewords of C. Prove that $d(C) = w(C)$.* [7]

(c) Laat C die ternêre lineêre kode wees met voortbringermatriks / *Let C be the ternary linear code with generator matrix*

$$H = \begin{bmatrix} 1011 \\ 0112 \end{bmatrix}$$

i. Lys die kodewoorde van C. / *List the codewords of C.* [3]

ii. Bepaal die minimum afstand van C. / *Determine the minimum distance of C.* [1]

iii. Is C 'n perfekte kode? (Gee redes). / *Is C a perfect code? (give reasons).* [2]

iv. Vind 'n pariteitskontrolematriks vir C. / *Find a parity–check matrix for* C. [2]

(5) (a) Veronderstel C is 'n $[n, k]$–kode oor $GF(q)$. Bewys dat / *Suppose* C *is an* $[n, k]$*–code over* $GF(q)$. *Prove that* [8]

i. elke vektor van $V(n, q)$ is in 'n neweklas van C. / *every vector of* $V(n, q)$ *is in some coset of* C.

ii. elke neweklas bevat q^k vektore. / *every coset contains* q^k *vectors.*

iii. twee verskillende neweklasse is disjunk. / *two distinct cosets are disjoint.*

(b) Laat C die binêre lineêre kode wees met voortbringermatriks / *Let C be the binary linear code with generator matrix*

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

i. Stel 'n dekoderingstabel vir C op. / *Write down a decoding table for C.* [4]

ii. Vind 'n standaardvorm pariteitskontrolematriks vir C en skryf die pariteitskontrole vergelykings van C neer. / *Find a standard form parity-check matrix of C and write down the parity–check equations for C.* [3]

iii. Stel die sindroom opsoektabel van C op. / *Write down the syndrome look–up table for C.* [2]

iv. Vind die sindrome van die ontvangde vektore 11101 en 01111, en dekodeer hulle. / *Find the syndromes of the received vectors 11101 and 01111, and decode them.* [2]

(6) (a) Veronderstel C is 'n $[n,k]$–kode oor $GF(q)$ met pariteitskontrolematriks H. Bewys dat die minimum afstand van C gelyk is aan d as en slegs as enige $d-1$ kolomme van H lineêr onafhanklik is, terwyl daar d kolomme is wat lineêr afhanklik is. / *Suppose C is an $[n,k]$–kode over $GF(q)$ with parity–check matrix H. Prove that the minimum distance of C is equal to d if and only if any $d-1$ columns of h are linearly independent, while there are d columns that are linearly dependent.* [10]

(b) Vind 'n pariteitskontrolematriks vir $Ham(3,3)$. Hoeveel kodewoorde het $Ham(3,3)$. / *Find a parity–check matrix for* $Ham(3,3)$. *How many codewords does* $Ham(3,3)$ *have.* [4]

(c) Vind 'n pariteitskontrolematriks vir $Ham(3,2)$ en dekodeer 1110110. / *Find a parity–check matrix for* $Ham(3,2)$ *and decode 1110110.* [5]