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

Universiteit van Stellenbosch
Toegepaste Wiskunde 314
Semestertoets II
12 Junie 2004
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	/21	J. van Vuuren
2	/19	J. van Vuuren
3	/15	P. Grobler
4	/29	P. Grobler
5	/8	P. Grobler
6	/8	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) Verduidelik die verskil tussen 'n *onreduseerbare* polinoom en 'n *primitiewe* polinoom in die ring $(\mathbb{Z}_2, +, \times)$. / *Explain the difference between an* irreducible *polynomial and a* primitive *polynomial in the ring* $(\mathbb{Z}_2, +, \times)$. [2]

(b) Gebruik **Mathematica** om te toets of die volgende polinome primitief is in die ring $(\mathbb{Z}_2, +, \times)$, of nie. Motiveer volledig. / *Use* **Mathematica** *to determine whether the following polynomials are primitive in the ring* $(\mathbb{Z}_2, +, \times)$*, 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) Gebruik die feit dat die generator–funksie $G(x) = \sum_{i=0}^{\infty} s_i x^i$ wat ooreenstem met 'n binêre stroom $\underline{s} = s_0, s_1, s_2, \ldots$ geskryf kan word as $G(x) = \Psi(x)/f(x)$, waar $\Psi(x)$ 'n polinoom van graad hoogstens $m-1$ in die ring $(\mathbb{Z}_2, +, \times)$ is, en $f(x) = \sum_{i=0}^{m} p_i x^i \in (\mathbb{Z}_2, +, \times)$ die karakterestieke polinoom is van 'n linêre terugvoer skuifregister $\mathcal{F}^m_{f(x)}$ wat $\underline{s}$ genereer, om te bewys dat indien $f(x)$ onreduseerbaar is met eksponent e in die ring $(\mathbb{Z}_2, +, \times)$ en $\underline{s} \neq 0, 0, 0, \ldots$, die periode van $\underline{s}$ presies e is. / *Use the fact that the generator function* $G(x) = \sum_{i=0}^{\infty} s_i x^i$ *associated with a binary stream* $\underline{s} = s_0, s_1, s_2, \ldots$ *may be expressed as* $G(x) = \Psi(x)/f(x)$, *where* $\Psi(x)$ *is a polynomial of degree at most* $m-1$ *in the ring* $(\mathbb{Z}_2, +, \times)$, *and* $f(x) = \sum_{i=0}^{m} p_i x^i \in (\mathbb{Z}_2, +, \times)$ *is the characteristic polynomial of a linear feedback shiftregister* $\mathcal{F}^m_{f(x)}$ *that generates* $\underline{s}$, *to prove that if* $f(x)$ *is irreducible with exponent* e *in the ring* $(\mathbb{Z}_2, +, \times)$ *and* $\underline{s} \neq 0, 0, 0, \ldots$, *then the period of* $\underline{s}$ *is exactly* e. [6]

(daar is nog plek om u antwoord op die volgende bladsy voor te sit . . . / *there is additional space overleaf to continue your answer* . . .)

(d) Gee 'n interpretasie van die betekenis van die funksie $\Psi(x)$ in vraag (c), in die konteks van die lineêre terugvoer skuifregister $\mathcal{F}^m_{f(x)}$. / *Interpret the meaning of the function* $\Psi(x)$ *in question (c), in the context of the linear feedback shiftregister* $\mathcal{F}^m_{f(x)}$. [2]

(e) Die binêre stroom $\underline{s} = 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, \ldots$ is deur middel van 'n lineêre terugvoer–skuifregister, $\mathcal{F}^4_{f(x)}$, gevorm. Gebruik tegnieke uit *lineêre algebra* om die terugvoer–polinoom $f(x)$ te bepaal. / *The binary stream* $\underline{s} = 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, \ldots$ *was formed by means of a linear feedback shift register,* $\mathcal{F}^4_{f(x)}$. *Use techniques from linear algebra to determine the feedback polynomial,* $f(x)$. [6]

(2) (a) Formuleer, sonder bewys, *Fermat se Klein Stelling.* / *Furmulate, without proof,* fermat's Little Theorem. [2]

(b) Gebruik *Fermat se Klein Stelling* as uitgangspunt en bewys die RSA–sisteem altyd korrek sal werk, met ander woorde dat die dekripsie van die enkripsie van enige versyferde skoonteks, x, weer x is. / *Use* Fermat's Little Theorem *as a point of departure, and prove that RSA system will always function correctly, in other words that the decryption of the encryption of any enumerated plaintext, x, is again x.* [6]

(c) Gebruik *Pollard se Algoritme*, die *Gewysigde Euklidiese Algoritme* en die *Kwadreer–en–Vermenigvuldig Algoritme* om die betekenis van die boodskap 4 026, wat met behulp van die RSA–sisteem deur Persoon A geënkripteer en digitaal onderteken is, en eintlik vir persoon B bedoel is, te ontsyfer. Wys al u werking duidelik. / *Use* Pollard's Algorithm*, the* Revised Euclidean Algorithm *and the* Square–and–Multiply Algorithm *to unravel the meaning of the message* 4 026*, which was encrypted and digitally signed via the RSA system by Person A, and which is actually meant for Person B.* [11]

Persoon / *Person*	n	e
A	7 081	701
B	7 031	607

(daar is nog plek om u antwoord op die volgende bladsy voor te sit . . . /
there is additional space overleaf to continue your answer . . .)

(3) (a) Definieer die Hamming afstand $d(\mathbf{x}, \mathbf{y})$ tussen twee vektore $\mathbf{x}$ en $\mathbf{y}$ van $(F_q)^n$.
Define the Hamming distance $d(\mathbf{x}, \mathbf{y})$ *between two vectors* $\mathbf{x}$ *and* $\mathbf{y}$ *of* $(F_q)^n$. [1]

(b) Bewys dat $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$ vir alle $\mathbf{x}, \mathbf{y}, \mathbf{z} \in (F_q)^n$.
Prove that $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$ *for all* $\mathbf{x}, \mathbf{y}, \mathbf{z} \in (F_q)^n$. [3]

(c) Bewys dat binêre (n, M, d)-kodes met die volgende parameters nie bestaan nie.
Prove that binary (n, M, d)*-codes with the following parameters do not exist.*

i. $(5, 3, 4)$ [3]

ii. $(8, 30, 3)$ [2]

(d) i. Wys dat 'n ternêre $(3, M, 2)$–kode $M \leq 9$ moet hê.
Show that a ternary $(3, M, 2)$*–code must have* $M \leq 9$. [4]

ii. Vind 'n ternêre $(3, 9, 2)$–kode . / *Find a ternary* $(3, 9, 2)$*–code* . [2]

(4) (a) Gestel C is 'n nie-triviale deelruimte van $V(n, q)$. Bewys dat enige voortbringerversameling van C 'n basis van C bevat. / *Suppose* C *is a non-trivial subspace of* $V(n, q)$. *Prove that any generating set of* C *contains a basis of* C. [6]

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

$$H = \begin{bmatrix} 1011 \\ 2201 \end{bmatrix}$$

i. Lys die kodewoorde van C. / *List the codewords of C.* [2]

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]

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

$$G = \begin{bmatrix} 10011 \\ 01101 \end{bmatrix}$$

i. Met behulp van neweklasse, stel 'n dekoderingstabel vir C op.
With the aid of cosets, draw up a decoding table for C. [6]

ii. Vind die standaardvorm pariteitskontrolematriks H van C.
Find the standard form parity–check matrix H of C. [2]

iii. Skryf die pariteitskontrolevergelykings van C neer.
Write down the parity–check equations of C. [3]

iv. Stel die sindroom opsoektabel van C op.
Draw up the syndrome look–up table of C. [3]

v. Dekodeer die vektore 11111 en 10101. *Decode the vectors 11111 and 10101.* [4]

(5) (a) Skryf die pariteitkontrolematriks H vir $Ham(3,2)$ in leksikografiese orde neer.
Write down the parity-check matrix H for $Ham(3,2)$ in lexicographic order. [2]

(b) Gebruik $Ham(3,2)$ om die ontvangde vektor 1011101 te korrigeer. *Use $Ham(3,2)$* to decode the recieved vector 1011101 . [2]

(c) Gebruik die matriks H in (a) om die pariteitkontrolematriks $\hat{H}$ vir die uitgebreide hammingkode $H\hat{a}m(3,2)$ neer te skryf.
Use the matrix H in (a) to write down the parity-check matrix $\hat{H}$ for the extended hamming code $H\hat{a}m(3,2)$. [2]

(d) Gebruik $\hat{H}$ om die vektor 10111001 te korrigeer.
Use $\hat{H}$ to decode the vector 10111001 . [2]

(6) Laat C die lineêre [10,8]–kode oor $GF(11)$ wees met pariteitskontrolematriks
Let C be the linear [10,8]–code over $GF(11)$ with parity–check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{bmatrix}.$$

(a) Skryf die sindroom $S(\mathbf{y})$ neer van die vektor $\mathbf{y} = y_1 y_2 \dots y_{10}$.
Write down the syndrome $S(\mathbf{y})$ of the vector $\mathbf{y} = y_1 y_2 \dots y_{10}$. [2]

(b) Neem aan dat 'n enkelfout van grootte k in posisie j van 'n kodewoord $\mathbf{x}$ gemaak was. Vind die sindroom van die resulterende vektor $\mathbf{y}$.
Assume that a single error of magnitude k was made in position j of a codeword $\mathbf{x}$. Find the syndrome of the resultant vector $\mathbf{y}$. [2]

(c) Gebruik C om die ontvangde vektore 0617960587 en 3617960587 te dekodeer.
Use C to decode the received vectors 0617960587 and 3617960587. [2]