ENIGE (SAK)REKENAARS TOEGELAAT

University of Stellenbosch
Toegepaste Wiskunde 314
Semestertoets 1b
24 Maart 2004 om 19:30
Time: 90 min *Full marks*: 40

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	/15	H Botha
2	/15	H Botha
3	/10	H Botha
Totaal		

Eksaminatore / Examiners: Dr PJP Grobler & Prof JH van Vuuren

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 moet in ink direk op hierdie vraestel/antwoordstel ingevul word.

(7) Hierdie vraestel/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 must be supplied in ink directly on this question/answer paper.

(7) Before leaving the examination room candidates must hand this question/answer paper 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

Toegepaste Wiskunde 314: Semestertoets 1b, 2004

1.1 Toegepaste Wiskunde 314: Semestertoets 1b, 2004

(1) Die onderstaande kriptoteks is deur middel van die affiene substitusie $\aleph_{26}^{a,b}$ gevorm. / *The ciphertext below was formed by means of the affine substitution* $\aleph_{26}^{a,b}$.

```
UZSGHBMEITVMMHMEITVYKENULFMZVMEHKVMEHFMIUHTEKKQTSSLQUZMMZEHWGHEQTUKCML
LUKTEKRESLEHLMKKSHKCTEQTTMTUBXZSWUIMKENVSUIMVTEZVMMHTMULKSTUBZMLEIESGK
MBGQUVESHUVTSWMCTMZMTMCUKVUGITVPGBUEKWVCSYMUZKLUVMZTMMHVMZMBVTMLGEVDSL
BIYWHUKEGWUHBUXVMZVTEKTEKZMLEIESGKMBGQUVESHCUKIERMHUVKQTSSLTMKVGBEMBWU
VTMWUVEQKEHDUZVEQGLUZVTMQULQGLGKFMIEHHEHIUZSGHBMEITVMMHHEHMVYSHMEHMEIT
VMMHHEHMVYXSGZMEHKVMEHKXUWELYWSRMBVSWELUHFGVMEHKVMEHZMWUEHMBEHWGHEQTEH
MEITVMMHHEHMVYXERMMEHKVMEHXUELMBUHMNUWEHUVESHVTUVCSGLBTURMULLSCMBTEWVS
KVGBYXSZUBEDLSWUUKUHMLMQVZEQULMHIEHMMZUVVTMMEBIMHSKKEKQTMVMQTHEKQTMTSQ
TKQTGLMEHJGZEQTMEHKVMEHZMHSGHQMBIMZWUHQEVEJMHKTEDEHMEITVMMHHEHMVYKENUH
BCUKVSFMKVUVMLMKKXSZUHGWFMZSXYMUZKTMBEBHSVMRMHUDDLYXSZKCEKKQEVEJMHKTED
GHVELMEITVMMHHEHMVYHEHMQEVEJMHKTEDFMEHIIZUHVMBEHHEHMVMMHTGHBZMBUHBSHMX
SLLSCEHIVTMXUELEHISXVTMMHVZUHQMMNUWVSVTMMVTMEHKVMEHUVVMHBMBKMQSHBUZYKQ
TSSLUVUUZUGDLUHHEHIVSGKMVTEKZSGVMVSMHVMZVTMMVTEHJGZEQTCTELMUVUUZUGTMCZ
SVMUHMKKUYXSZCTEQTTMCUKSHLYIERMHULEVVLMUFSRMTULXWUZAKEHCTEQTTMCZSVMSXT
EKDLUHKXSZVTMXGVGZMEXECMZMVSTURMVTMISSBXSZVGHMVSDUKKWYMNUWEHUVESHKECSG
LBISVSJGZEQTECSGLBKVUYVTMZMXSZXSGZYMUZKEHSZBMZVSKVGBYWUVTMWUVEQKUHBDTY
KEQKEEWUIEHMWYKMLXFMQSWEHIUVMUQTMZEHVTSKMFZUHQTMKSXVTMHUVGZULKQEMHQMKQ
TSSKEHIVTMVTMSZMVEQULDUZVSXVTMWTMZMUZMVTMZMUKSHKCTEQTLMUBWMVSVTEKDLUHU
FSRMULLEVEKWYBEKDSKEVESHXSZUFKVZUQVUHBWUVTMWUVEQULVTSGITVUHBWYLUQASXEW
UIEHUVESHUHBDZUQVEQULUFELEVY
```

(a) In watter natuurlike taal is die onderliggende skoonteks na alle waarskynlikheid? Motiveer volledig. / *What is the probable underlying natural language of the associated plaintext? Motivate fully.* [3]

(b) Stel die drie waarskynlikste sisteme van twee gelyktydige lineêre kongruensies op waarmee u die sleutel–parameters a en b sou kon oplos. Motiveer die volgorde waarin u die sisteme sou oplos. / *Formulate the three most likely systems of two simultaneous linear congruences from which you would solve for the key parameters a and b. Motivate the order in which you would go about solving the systems.* [3]

(c) Los u sisteme in (b) op. Wys alle werking. / *Solve your systems in (b). Clearly show your working.* [6]

(d) Dekripteer die kriptoteks met die sleutelpare, soos in (c) verkry. Watter van hierdie sleutelpare is korrek? Motiveer deur die eerste 15 karakters van die skoonteks te gee. / *Decrypt the ciphertext, using the resulting key parameter pairs, as found in (c). Which of the pairs is correct? Motivate by producing the first 15 characters of the associated plaintext.* [3]

(2) Die onderstaande kriptoteks is deur middel van die Vigenère substitusie $\vartheta_{26}^{n,\underline{s}}$ gevorm. / *The ciphertext below was formed by means of the Vigenère substitution* $\vartheta_{26}^{n,\underline{s}}$.

```
ZROVIOVMYJXPZRDLGNVIOVHHZXSYMDGPLEKCRHFRXTEKTERTEIEVIYYYYUVPUEDRXPRGSVV
ZWQLKLPDEEZGDRROGLJJMNJSYVSQYMDWVTVROJEEVXSNEDDECTIWXVZJWXRRYNLZNEDZREY
IDRQPTPLJWLJITEWEVMYVMYJXPZREIMPUXZFFERMYRTZJXHIMEZRRKSSLVHZXKNLZYIWUSF
KWZDISFTPFJLGSDZXTFRMLXYFXSZRRTEXVSQZXEYVPVSQVMYJXPZRDWIWCSHJXFUIYKWTEG
WLHTEKRISDJQLERHVVPRTAFMYKIORWDZWERREJEEVXSZRKLVTTLMLXNCILIPJVMYJXPZRSR
HYFXTDTCVWDVHPESFXLLEHDKMWCMYEMYVXPVRSLROIIORROFRPYIHRWHIMEZRRISFEHFEMG
VVDZXTVWTEXSVLZGIZWSMKETEMYXEUFFMLXHZXSFYEJYNTIDJLPUMODEYRKPKSLMSTUWHZW
DDMWZXLICDVVGZGPFREYIRISFEHDKLLKLPYEOWPLKJPVXLEHGRVTTSDVZPZRDSCXZHYZRPK
IPELFEHCVHLEHZEISVLLUEEVQAFVLICUFFLJEEVENYICKILTLTEKXRXSVQLKMNJEEKLPKIN
YRTTEWYMRYWNYSZCMYNMYKICKLFIECFYYUXSZWEZQPYIHISEVMSRZPXMGVRFGXSVEXSMEZS
YKSRVXEFEFEMGVVDZXJRRZKLPIXPDTZIECPTZJMEZSYKILTLTEKTEEAIMGRXPJGSFSWZRDT
LLWJSRYDVRQFPWFAPUXSVRRISDJQLERDWEEYICKVTVHEFLPCTPZRDKITEKPKEUFFMPVPTSX
DIYUMYXLTDXZKLPUMCVGEFVZWXSVTLKIYKSQWMNVMYSICEITEWEVMYNEDRTAFMYKIORWLKI
NYRTTEWVBAVVEKLTIHNCEDJITEWEVMYNSCBIOZREYMDGEEVREFJQZGPWVZDRTEIEVIYYYYU
VPUEYUXHFXZEMYVXPVRSLROIIORROEMYVLZCHTEKLKIXGSCRVJGSDKASVRSVALJJTIWERTA
FMYKIOSYESCYZRPKIPELFEHCVHLEHQFYCKLPGSDZXTFRHRWXRHPGICDEYVRERROZRYZRPKI
PELFEHCVHLEHDZBSVALJTCFQZKIOKSEVGSEMNRPPOTPIXDVGZEHNCEDJASZPPZREYIMVVYG
EEVREFJQZGPYINFQACIEVHLEEDKSYZWSZRRIEYXIZWXSVSCVXTTEWGLJJMNJTFSPTTEEZSY
JACZXEVRTELTJWARVPKMXVATKLZLXEYIMVRPWMEFJNCSDVGZEXLTXHZXSJGTVREZJTTPTKI
CRXFIIZIGZCPPRKFVWPZRDKITEILIRPUEOFGEFVLKIQISXKLPLRTMICJMEPSQQYCZGSZRYZ
RPKIPELFEHCVHLEHQZZPWSCRXSVWTJSYRRPNHPKICDMYRXTFRZWQZCINLPLIHTDIYJMZEWS
VHPUMNRXPUXSVXSVWTJXZXVZJWXRRY
```

(a) Voer 'n volledige Kasiski analise op die kriptoteks uit om die waarskynlike sleutellengte, n, te bepaal. Motiveer u werking, en toon die inhoud en posisies van enige teksstringe wat gebruik word. / *Conduct a full Kasiski analysis of the ciphertext to determine the probable key length,* n. *Motivate your reasoning, and show the contents and positions of any text strings you use.* [5]

(b) In watter natuurlike taal is die onderliggende skoonteks na alle waarskynlikheid? Motiveer volledig. / *What is the probable underlying natural language of the associated plaintext? Motivate fully.* [3]

(c) Gebruik letterfrekwensies om die sleutel, $\underline{s}$, te bepaal. Wys al u werking. / *Use letter frequencies to determine the key,* $\underline{s}$*. Show all your working.* [6]

(d) Dekripteer die kriptoteks met die sleutel in (c) gevind. Wat is die eerste 10 karakters van die onderliggende skoonteks? / *Decrypt the ciphertext with the key found in (c). What are the first 10 characters on the associated plaintext?* [1]

(3) Die onderstaande kriptoteks is deur middel van die Hill transposisie $\mathcal{H}_{26}^{n,\mathbf{S}}$ gevorm. / *The ciphertext below was formed by means of the Hill transposision* $\mathcal{H}_{26}^{n,\mathbf{S}}$.

`KYAXBKKXONGZHNKVALXOYVOL`

(a) Gestel dit is bekend dat die skoonteks `alberteinsteinisinzurich` onder die sleutel $\mathbf{S}$ na `WVYCBONRBXSJHUZNVVXZOLZB` enkripteer. Gebruik 'n bekende (skoonteks, kriptoteks)–paar aanval om die sleutel, $\mathbf{S}$, te vind. Wys al u werking. / *Suppose it is known that the plaintext* `alberteinsteinisinzurich` *encrypts to* `WVYCBONRBXSJHUZ NVVXZOLZB` *under the key* $\mathbf{S}$. *Launch a known (plaintext, ciphertext)–pair attack to solve for the key,* $\mathbf{S}$. *Show all your working.* [9]

(b) Gebruik die sleutel in (a) om die bostaande kriptoteks, wat met behulp van dieselfde sleutel gevorm is, te dekripteer. / *Use your key in (a) to decrypt the above ciphertext, which was formed, using the same key.* [1]