Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaaltoets 3: Donderdag 4 Maart 2004

MEMORANDUM

Tuttoets 1a.

Sien asseblief die uitgedeelde addisionele klasnotas.

Tuttoets 1b.

Indien 'n Kasiski–analise op die kriptoteks uitgevoer word,word die volgende lys van herhalings van lengte minstens 6 karakters verkry:

Teksstring	Posisies	Afstand(e)	Faktorisering(s)
EANVLEVFNZFEKQ	70, 163	93	3×31
IFUDTEIK	355, 694	339	3×113
EYMNUJEU	450, 747	177	3×59
XATLOIA	233, 833	600	$2^3 \times 3 \times 5^2$
NLEBVJS	207, 471	264	$2^3 \times 3 \times 11$
GJODASV	274, 595	321	3×107
EMMSWRJ	580, 760	180	$2^2 \times 3^2 \times 5$
FUDTEI	383, 512, 821	129, 309	3×43, 3×103
DAIYEI	680, 689	9	3^2

Die sleutellengte, n is dus na alle waarskynlikheid 3. Die oorspronklike kriptoteks word dus in die volgende 3 subtekste verdeel:

Subteks 1:

```
KRZGZRVKZVERPUKWCIFKEEVEVVZKFUJKRVEVZYFZFYVIITYSIZRZJYEVVZKZITKJICVCXL
VIRRVZJVTIRFWRVVPEFETGDVVTZFLVISVFJVDKGTJXNILVFTIDIKCPTKJVDIUZZIJYRFEF
JXVVCRVRRFYUUUWUZLVZYVWLRNTZVCUDIVJMYYGUYLIZZVKYVDRVRESJJFGDVKVPFXIUEJ
PRYUKESKFJAKSZTVEIIUIIDIVIFVZKKFVVFEVFIYUUXESJKIVSIXIRTVKFYTGRFCDIVPTI
RFZIRRIICWREZSGXJZKZVIYJMZFKELVYIKEKPELF
```

Subteks 2:

```
ZOFAFLEOUNLDDLZSGKFOLAAALFFQMGFDNNSFFWSFXWFSKAWSQHOLAAALFFQPADZWWAGSWE
JWJTSLLXLALFJGLFFWWGGJALKMLXJFKSVVLUHWJWAHWWAVXLFTKAKJCKLFTGALFWWWUJYD
XMLQTTLLUFMJSXLALEJFWSMJFLZIUDFTXDAWAWSKWSSUWAGWSGDTAMWZKOJATLUHDQGUWA
KQWGZMWZJLMTSFGKDYSDYFTKJWEFFZHHMLZVVLWMJVAMWFWAKSASSLTSZMAGMLFFTLGXLA
LFDWAZVGWGDYEMJJKCZFYKWWWKEZYEJWAKGZUUFF
```

Subteks 3:

```
EESRGTPHHEULEOELFAEEYNNNENEFREOEEEDTTCTGTGELAPRRCRRENSNENESATEECTFFRNB
SMKLSIHAOZIOSNWTIDSTMOSHERYCRTASCEHOUROSNORQRTAOUESLKOEAHUEFGSCATFTIFK
IRHLELOTKENENIYGNBSTNRTEEENUAEUEIDEWCXNTQDTSVNTRLFGRCMRAHNOSUHRTOCWAAL
TAAFEMREISSYSGDOAENAEUEWECMDGAELSWURTHENEITMROSVTRNDMIRKRGNMTIAUEHRAOS
IWLMNAPBMROTETOELEETETMLSSEINBTOSKWEAOT
```

Vir hierdie ry subtekste lyk die letterfrekwensie tellings soos volg:

	1	2	3		1	2	3		1	2	3
A:	1	30	21	J:	17	18	0	S:	8	20	24
B:	0	0	4	K:	24	17	6	T:	13	12	31
C:	8	2	10	L:	8	33	13	U:	14	10	10
D:	9	13	7	M:	2	14	11	V:	46	7	2
E:	19	7	50	N:	2	3	24	W:	5	36	7
F:	24	34	9	O:	0	5	20	X:	7	8	1
G:	7	17	9	P:	7	1	3	Y:	16	6	4
H:	0	6	11	Q:	0	6	2	Z:	26	14	1
I:	34	1	13	R:	23	0	26				

Die bogenoemde geblokte hoë letterfrekwensies dui daarop dat die skoonteks letter `e` soos volg enkripteer:

Subteks	Kripto–Karakater	Kodeletter
1	`V`	`R`
2	`W`	`S`
3	`E`	`A`

Die kriptoteks dekripteer met behulp van die kodewoord `RSA` na:

```
theaweinspiringattemptwhicheventuallyledtothefallofrsaonetwentynineinn
ineteenninetyfourdoesnotleaveevenadentinthecoatingofthegeneralrsaciphe
rbarryciprawritesinhisnineteenninetysixaritclethesecretlifeoflargenumb
ersremarkableasitisthefactorizationofrsaonetwentyninedoesnotcompromise
thesecurityofcurrentrsabasedcodesthecomputerprocessingpowerrequiredtof
actornumbersstillskyrocketsasthenumberofdigitsincreasethefactoringfolk
sfiguretheyllbeabletoattackonehundredandfiftydigitnumbersinthenearfutu
reanewtechniquecallednumberfieldsievewhichexpandsthequadraticsieveinto
therealmofalgebraicnumbershasshownpromisebutthecryptologycrowdcaneasil
ystayaheadofthenumbertheoristsjustbybasingcodesonlargerandlargernumber
swererecommendingthatpeopleusetwohundredtothreehundreddigitnumbersnote
srivestbarringadramaticbreakthroughincomputationalnumbertheoryfactoris
ationwillremainahardproblemforalongtimebutprogresslikethentegersthems
elvesissomethingnumbertheoristsknowtheycancounton
```

oftewel na

“The awe–inspiring attempt which eventually led to the fall of RSA one twenty nine in nineteen ninety four does not leave even a dent in the coating of the general RSA cipher. Barry Cipra writes in his nineteen ninety six aritcle *The Secret Life of Large Numbers*: “Remarkable as it is, the factorization of RSA one twenty nine does not compromise the security of current RSA–based codes. The computer processing power required to factor numbers still sky–rockets as the number of digits increase. The factoring folks figure they’ll be able to attack hundred and fifty digit numbers in the near future – a new technique called *Number Field Sieve*, which expands the *Quadratic Sieve* into the realm of algebraic numbers, has shown promise. But the cryptology crowd can easily stay ahead [of the number theorists], just by basing codes on larger and larger numbers. ‘We’re recommending that people use twoo hundred to three hundred digit numbers,’ notes Rivest. Barring a dramatic breakthrough in computational number theory, factorisation will remain a hard problem for a long time. But progress, like the integers themselves, is something number theorists know they can count on.”’

ná invoeging van spasies.