Digital Security (Huygens College)

Opgave 1, Monday, November 21, 2010

Handing in your answers: There are two options:

1. Send your solutions by e-mail to `pim@cs.ru.nl` with subject '*opgave 1*'. This e-mail should only contain a single PDF document as attachment (unless explicitly stated otherwise). Before sending an e-mail make sure:
   - the file is a PDF document
   - your name is part of the filename (for example PimVullers_opgave-1.pdf)
   - your name and student number are included in the document (since they will be printed)
2. Put your solutions in Pim's post box (in the white cabinet near the printer at the station-side-end of the corridor on the second floor of the Huygens building). Before putting your solutions in the post box make sure:
   - your name and student number are written on the document

Deadline: Wednesday, December 1, 9:00 sharp!

Goals: After successfully completing this exercise you should be able to break simple substitution and transposition ciphers, and you know how to decrypt a Vigenère ciphertext.

Note: These tasks require that you study the material on substitution[1], transposition[2] and Vigenère [3] ciphers (Anderson[4], Section 5.2).

1. Break the mono-alphabetic substitution cipher (which is just a permutation of letters) of the ciphertext given below. The plain text, consisting of letters only, is in English.

   Explain briefly how you did it. [Note: 'I used a computer' is not accepted as an explanation.]

   Si spy net work, big fedjaw iog link kyxogy

2. Break the following transposition cipher. In a transposition cipher the characters are not changed but their position is permuted, for example the letter 'a' remains an 'a', only its position within the message changes. The plain text consists of letters only (no spaces), but is displayed here in groups of four for readability. Hint: the plain text (in English) is about **encryption**, so the word 'encryption' is likely to occur.

   Explain briefly how you did it. [Note: 'I used a computer' is not accepted as an explanation.]

   htsy nies ridd teun etei hpyt ryre lnon ewop elni onio wvrm roft tlts mgan iege rpcn teur auah pyex teer owvr fdrn aror ayno aroe eoyt ltvt

3. Decrypt the following Vigenère cipher text using the key 'rsa'.

   Explain briefly how you did it. [Note: 'I used a computer' is not accepted as an explanation.]

   kze dsgzu wfjdj srv kqlwadasy gsjafisgv

4. As an appendix you can find the NBV kerstpuzzel which contains some more code breaking assignments. Opgave 1 and 2 are encrypted using a mono-alphabetic substitution cipher and a transposition cipher, respectively. Both plaintexts are in Dutch. If you enjoyed the first two assignments you can have a look at the kerstpuzzel and try to break those ciphertexts.

---

[1] `http://en.wikipedia.org/wiki/Substitution_cipher`
[2] `http://en.wikipedia.org/wiki/Transposition_cipher`
[3] `http://en.wikipedia.org/wiki/Vigenere_cipher`
[4] `http://www.cl.cam.ac.uk/~rja14/Papers/SE-05.pdf`

NBV KERSTPUZZEL 7.12.2009

Wiskunde, Trudie
dat is niets voor vrouwen.
Dat moet je als studie
voor mannen beschouwen.
Jouw hoofd is – met ere,
ik wil je niet krenken –
om crème op te smeren,
maar niet om te denken.

Voor je ligt de NBV Kerstpuzzel van 2009, een fenomeen dat inmiddels haar 5-jarig jubileum viert, en aanleiding geeft tot veel zwoegen en zuchten (als een opgave even niet lukt), of juichen en fanatiek schrijven (als de oplossing van een opgave door begint te schemeren).

De volledige puzzel bestaat uit 6 vercijferde teksten, waarbij elke tekst een hint geeft voor het oplossen van de volgende. Beschrijvingen van vercijfersystemen zijn online beschikbaar (en kun je bijv. via google of wikipedia vinden).

Het eerste deel, waarin alle puzzels met de hand op te lossen zijn, sluit af met een vraag.

Echte fanatici kunnen door met het tweede deel van de puzzel, dat bestaat uit een paar lastigere vragen, waarbij handwerk niet altijd meer volstaat. Je kunt wel hulpmiddelen gebruiken zoals het programma Cryptool (hoewel we hebben gemerkt dat ‘oudere’ versies van Cryptool soms kleine foutjes in de ontcijferde teksten geven), of zelf programmeren. Ook deel 2 eindigt met een vraag.

De antwoorden op de 'tussenvraag' of de 'eindvraag' kun je mailen naar nbv@minbzk.nl onder vermelding van “NBV Kerstpuzzel 2009” en insturen tot uiterlijk 7 januari 2010 (helaas hebben we geen tijd om vragen te beantwoorden, dus je kunt alleen oplossingen opsturen).

Veel succes, maar vooral veel plezier gewenst, en als je het even niet ziet zitten, dan kun je je frustratie misschien nog omzetten in een mooi kunstwerk, zoals het werk hieronder, van een schilder die zelf ook nog een tijdje cryptoloog geweest is…

Ellen & Karin

NBV KERSTPUZZEL 7.12.2009

Opgave 1:

1 ½ ½ 6 ∞ ½√3 180 ½ ε ∞ e ½ ∞ i^2 ½ 100 1980 ∞ 180 2010 ½ 496 ∞ ε ½ ∞ ½ ½ 496 1729 1980 ½ ∞ 1 180 496 ε ½ ∞ 1 ½ ½ 100 ∞ 100 180 ½√3 ∞ 2010 180 180 496 ε -273.15 1980 ∞ ½ 496 ∞ 6 ½ 1980 1980 ½ 496 1729 ∞ 2010 ½ 496 2010 -273.15 100 ½√3 ½ 100 ∞ 8128 ½ 496 ε ½ 100 ∞ ε 180 180 496 ∞ ½√3 ½ 1980 -273.15 6 6 ½ 100 ∞ 180 ½√2 ∞ ε 180 180 496 ∞ -273.15 100 ε ½ 496 ½ ∞ 1729 12345 28 i^2 180 6 ½ 100 ∞ 8128 ½ 496 ε ∞ ½ 496 ∞ -273.15 6 ∞ 2010 ½ 496 0 (½ +½√5) e ½√2 ½ 496 ε ∞ ε 180 180 496 ∞ 6 ½ 1980 1980 ½ 496 1729 ∞ 1980 ½ ∞ 1 2009 1729 1729 ½ 6 ½ 100 ∞ i^2 (½ +½√5) e 2010 180 180 496 i^2 ½ ½ 6 ε ∞ 2^{128} 180 -273.15 6 1729 ∞ 1980 1 2009 0 12345 ε (½ +½√5) ε ½ 1729 ∞ 1729 0 1 496 (½ +½√5) e ½√2 1980 ∞ 180 2010 ½ 496 ∞ 1729 360 -273.15 496 1980 -273.15 -273.15 100 1729 ½ ∞ 180 180 496 6 180 ½√3 1729 2010 180 ½ 496 (½ +½√5) 100 ½√3 ∞ ε 180 180 496 ∞ 6 ½ 1980 1980 ½ 496 1729 ∞ 180 360 ∞ ½ ½ 100 ∞ 6 -273.15 100 ½√3 ½ ∞ 1729 1980 496 180 180 π ∞ 1980 ½ ∞ 1729 0 1 496 (½ +½√5) e 2010 ½ 100 ∞ ½ 100 ∞ ε ½ 2^{128} ½ ∞ 1729 1980 496 180 180 π ∞ 180 28 ∞ ½ ½ 100 ∞ 0 (½ +½√5) 6 (½ +½√5) 100 ε ½ 496 ∞ 1980 ½ ∞ 8128 (½ +½√5) π π ½ 6 ½ 100 ∞ π 2009 100 ∞ e (½ +½√5) e ∞ 180 100 1980 0 (½ +½√5) e ½√2 ½ 496 ½ 100 ∞ 2^{128} 180 100 ε ½ 496 ∞ ε ½ ∞ i^2 496 ½ ½ ε 1980 ½ ∞ 2010 -273.15 100 ∞ ε ½ ∞ 0 (½ +½√5) 6 (½ +½√5) 100 ε ½ 496 ∞ 1980 ½ ∞ 8128 ½ 1980 ½ 100 ?

NBV KERSTPUZZEL 7.12.2009

Opgave 2:

```
VTRAANTKEORGNLGEENOUETSERRVRDBOSBNVAOIRPLRAANPEUDEUMNDGSIAUIEHE
AHKTTKNESVATVETVTCENAALZASHDDLNWENYIRCSFODDSLIIVROEETDEJAIRABEE
IFRTDCRERSEIZEHEM
```

Opgave 3:

```
IDUETRTUDITTERDEIETREEUERRTTURETURRTUEDIETIRIIEEIITTRURURUDDRTR
TRUTRDITERTIEEERERURUDIRRDITTEIRUTETURRDUTUTTDITEEUEURIDURTTTEU
RIRUEIRUTTDTDIDEITRIETTRUUUUDEREETREETTTTTTRDURIRIRTRUETUDRERER
TRTRIEERTRIEUEEDIUTUTRDURITTRERUDDRTEIRTTERRTETIUURRDIRUUTRUDTR
TUUDTRDDIDURTTIDETIRURTRUTDRTUTDITIEIRTDUUURTEURURTEDDIEIRIRURT
RIEURTUDITTTRUTETUTREERITDEUUITITRITTUR
```

Opgave 4:

```
33024 99670 88766 67988 31415 88478 33757 78383 88830 80308
82908 74939 07643
```

Opgave 5:

```
NZATE ZQRQI MDFQA SWZNU AFINI LYXPC KJXWD CDUPL PPNEQ QSMHS
XPMIH OETOQ HKREC KTVNS LZSIA TGDVJ AXUXS QZYAW WSGIT NAXNU
CAGPL RMVLS MHNFK JDEDA FNNTL NCIBX HWAFF DMZBE BKAJS NXCEO
DDTXK GXVIJ UXEBR SSXHA GTBJO TDVIH EFQKC HAFEK IRZWP DIEYR
QSMWR ZNTJC NIYZQ GPJRW SEVIW XPFLX ESWTP PPHJN FANQE FHYGY
OEAMS QHQBJ KBJIY IWBIL TBPEZ UQFFT CRFGW BPOGD YIGGC HEPZL
QYGMX Z
```

Opgave 6:

```
213090351444552487871710875177965854787
                                      2
111934232051706745023473084710321088382
150183698659641458233362702907727479496
```

NBV KERSTPUZZEL 7.12.2009

- - - Eindvraag - - -

27 22 61 15 14 41 65 02 49 31 57 22 13 39 06 77 90 25 58 39 68

55 48 51 85 70 23 85 05 14 06 93 64 53 45 23 74 77 97 28 24 53

22 38 41 78 15 32 17 57 39 17 39 06 55 90 13 43 53 60 47 38 60

78 89 14 86 05 09 05 02 67 53 31 27 74 82 02 23 44 65 19 20 56

83 07 30 27 61 22 00 50 97 60 05 11 43 34 70 66 31 64 83 98 14

77 11 12 92 91 67 62 45 29 74 75 97 21 24 64 19 20 69 65 18 40

14 56 22 15 50 15 52 96 24 57 40 60 53 38 65 78 97 10 73 11 17

06 84 72 74 39 31 69 87 91 28 24 53 26 39 41 67 01 43 24 61 21

00 44 15 56 90 32 61 31 62 52 49 60 78 86 27 73 12 09 05 99 67

70 33 32 64 78 06