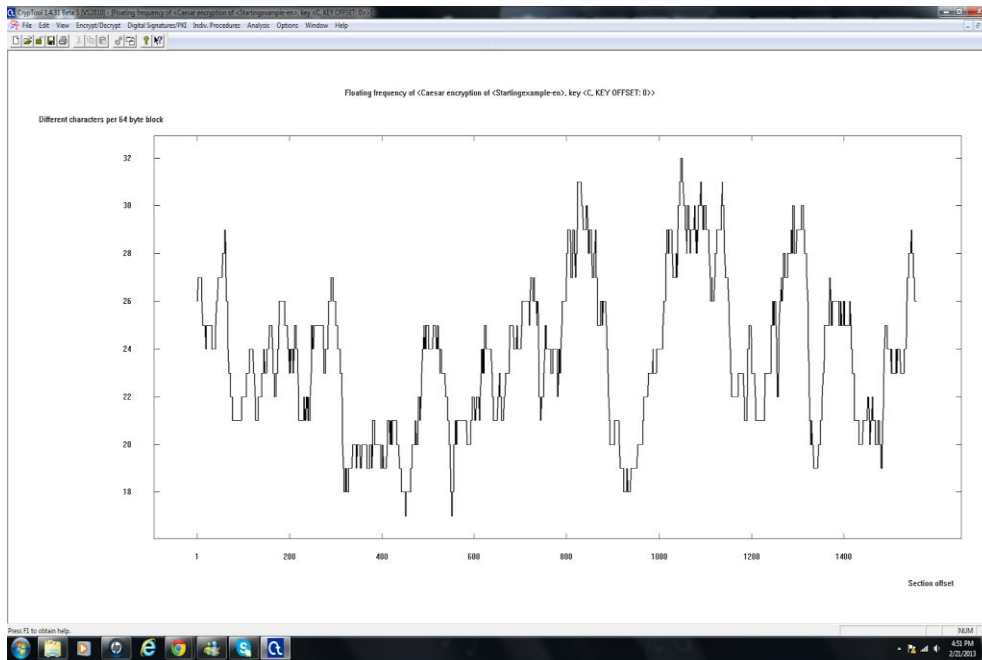
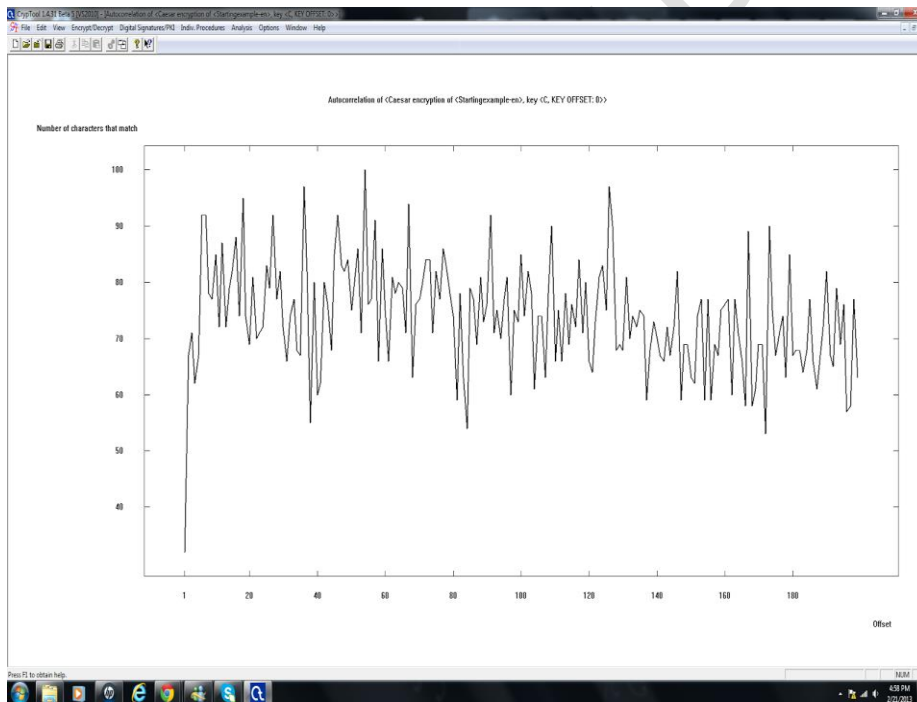




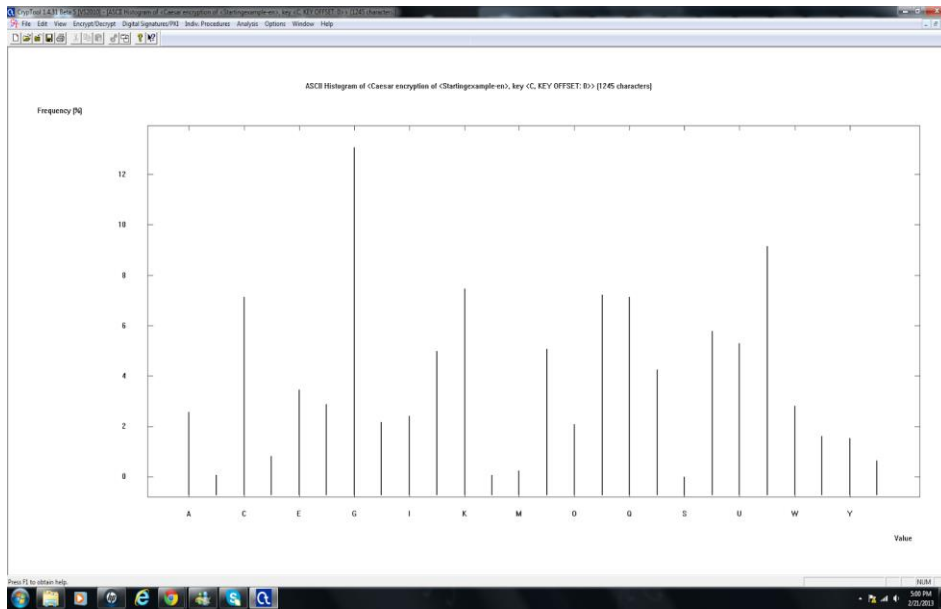
## The Floating Frequency



## AutoCorrelation



## Histogram

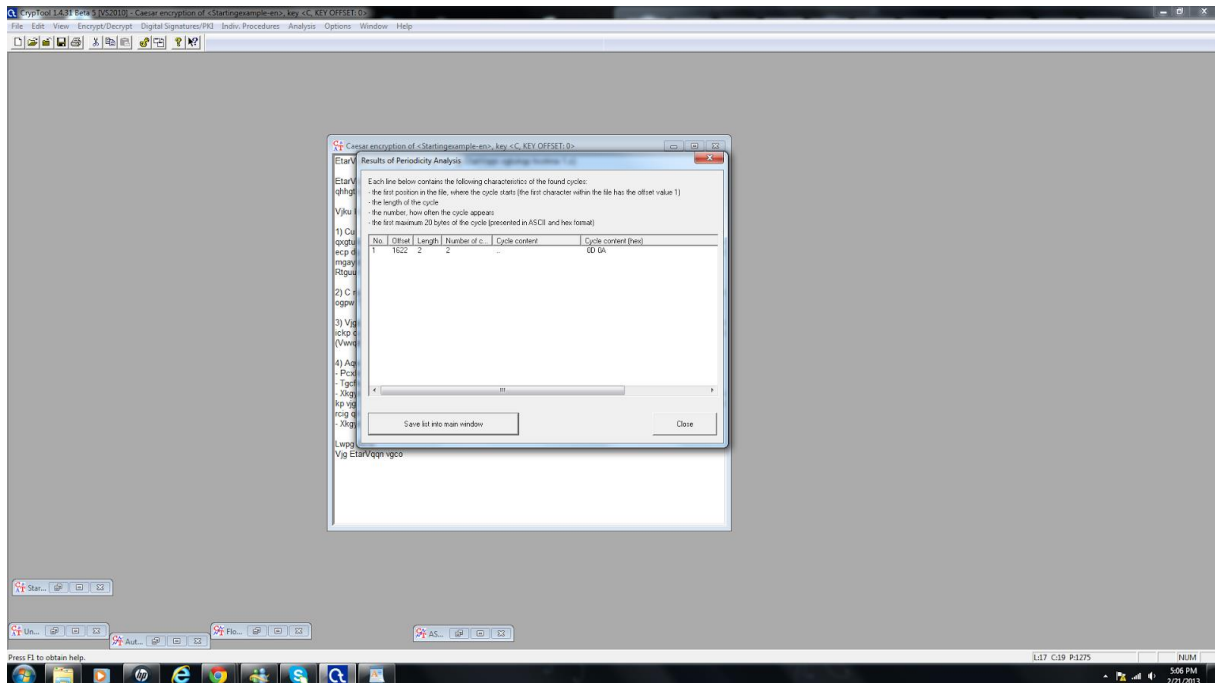


## N-Gram

N-Gram List of Caesar encryption of <Startingexample>.key <C, KEY OFFSET: 0>

No.	Character	Frequency (%)	Frequency
1	a	13.064	83
2	v	5.156	33
3	k	7.469	47
4	p	2.229	14
5	c	7.146	45
6	o	7.146	45
7	t	5.781	36
8	u	5.202	33
9	n	6.022	38
10	j	4.978	31
11	r	4.250	27
12	e	3.459	22
13	f	2.916	18
14	w	2.912	18
15	a	2.903	18
16	i	2.426	15
17	h	2.159	14
18	d	2.084	13
19	x	1.854	12
20	y	1.521	10
21	l	0.932	6
22	z	0.426	3
23	m	0.240	1
24	g	0.053	1
25	l	0.003	0

## Periodicity



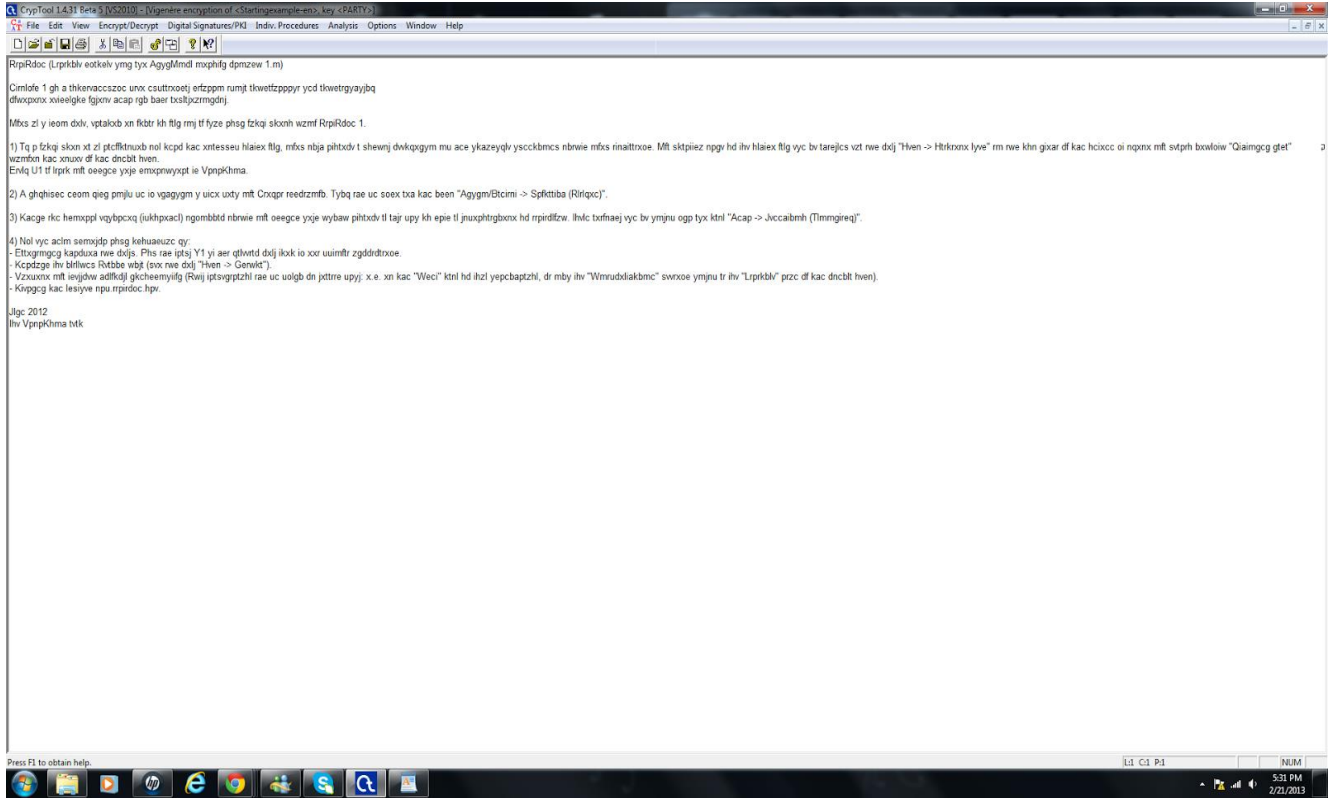
**Q1. The tool or technique from the above list that would be most effective for a cryptanalyst to use to decipher a text encrypted with the Caesar cipher:**

I think the most effective tool that a cryptanalyst could use would be the Histogram.

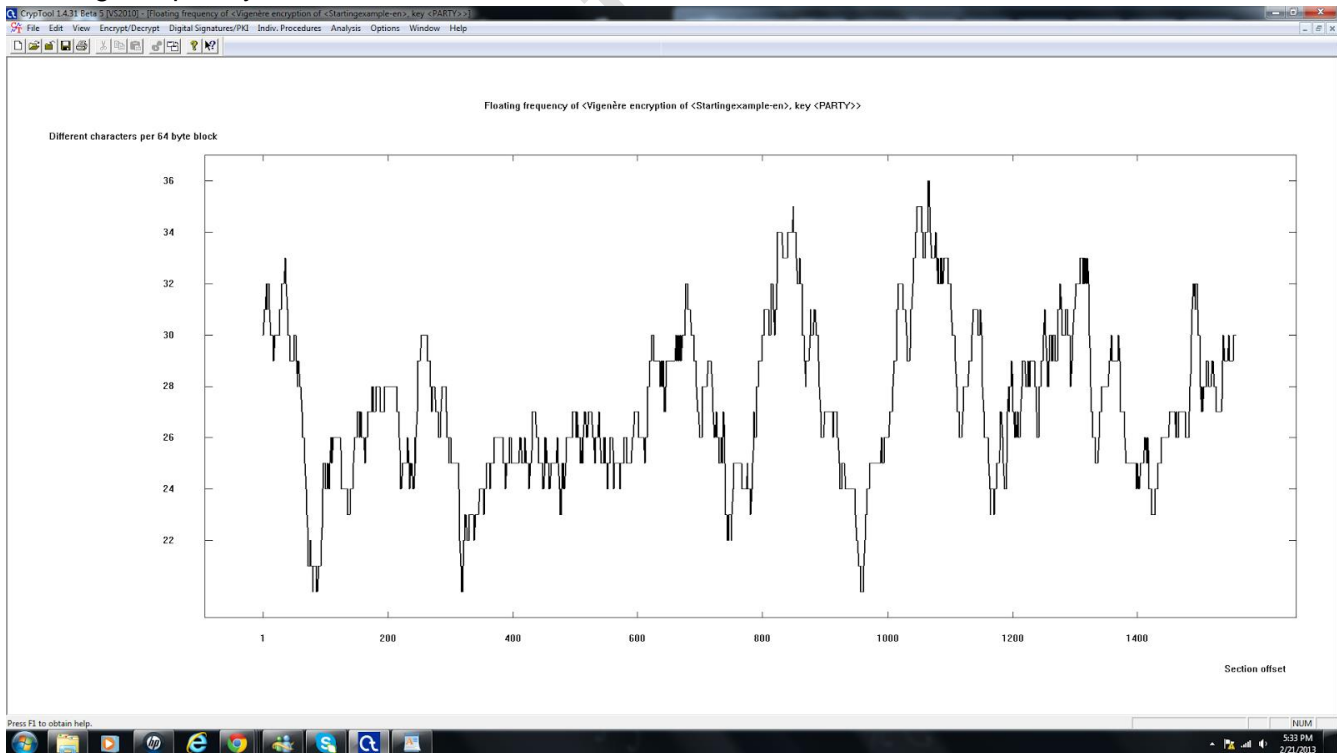
“*Cryptography* refers to the science and art of designing ciphers; *cryptanalysis* to the science and art of breaking them” (Anderson, R.,2008).This diagram shows the letters that are used and the frequency that they are and it shows the frequencies used. This also gives an idea about the way it is encrypted and can tell exactly which letters are used because of the comparing of the letters can be evident. In the Lab it states “ It is very useful for comparing the prevalence of different letters and can help derive the nature of the information and in some cases even reveal some of the character”'s representation.” (CSEC 630 Lab Assignment). In this technique you can see which letters are used and it would be most effective for a cryptanalyst to use.

**Vignere**

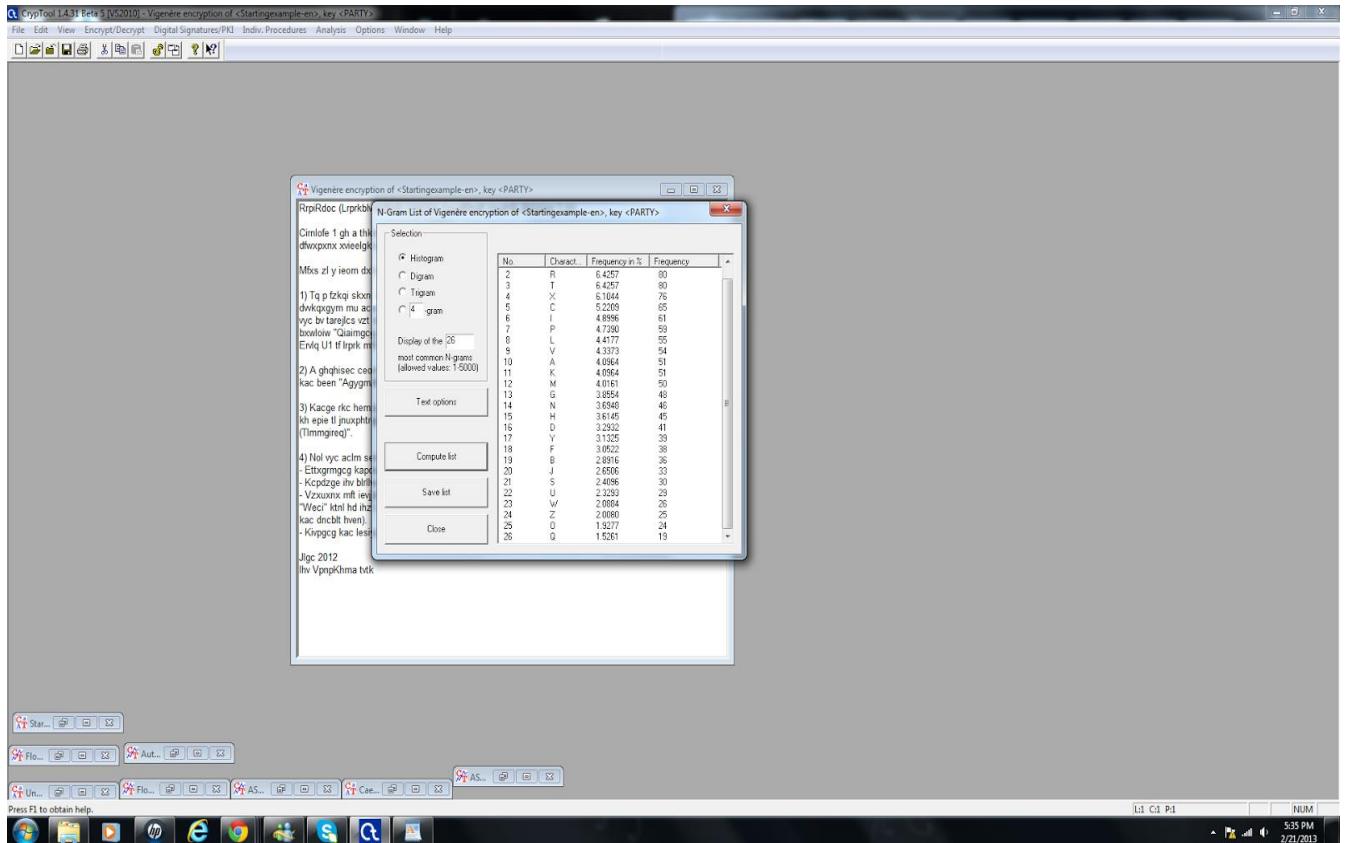
The Encrypted message



## Floating Frequency

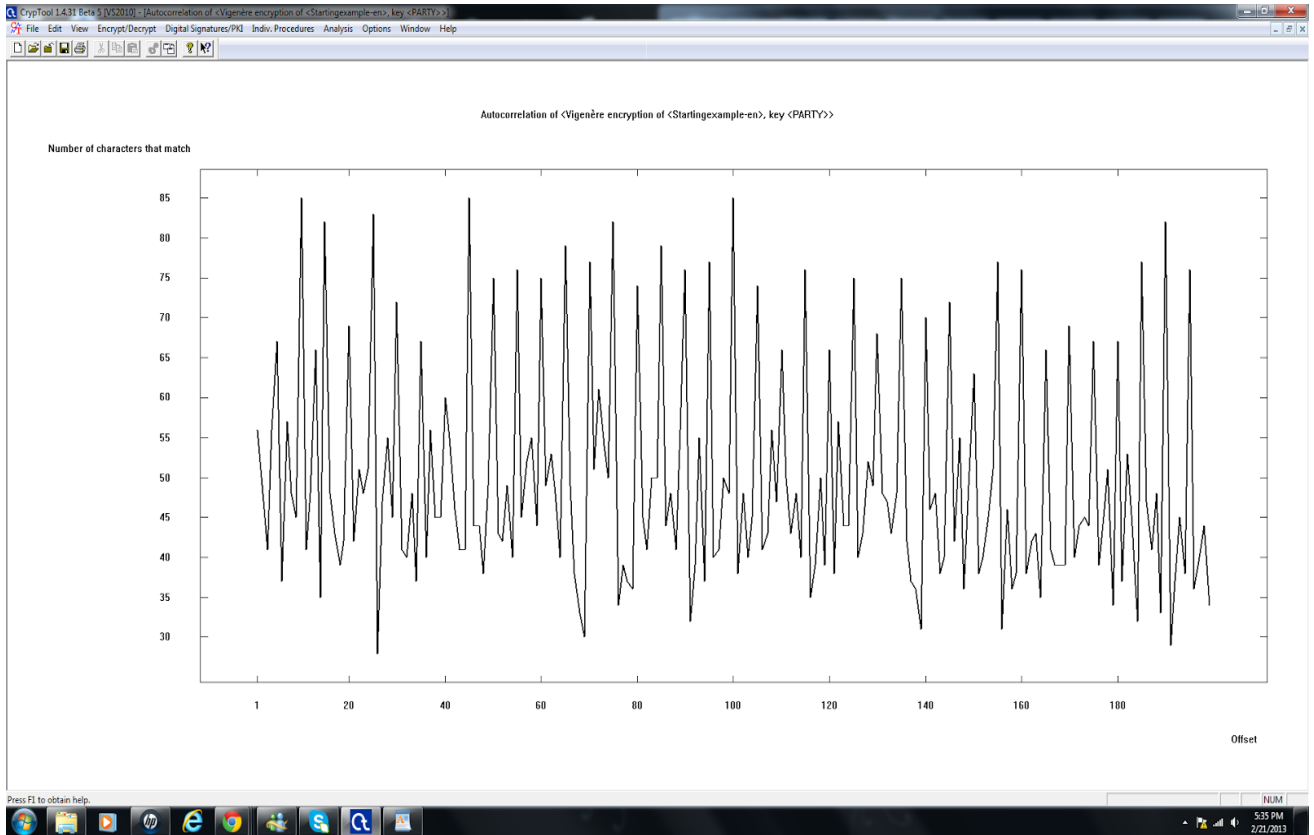


## N-Gram



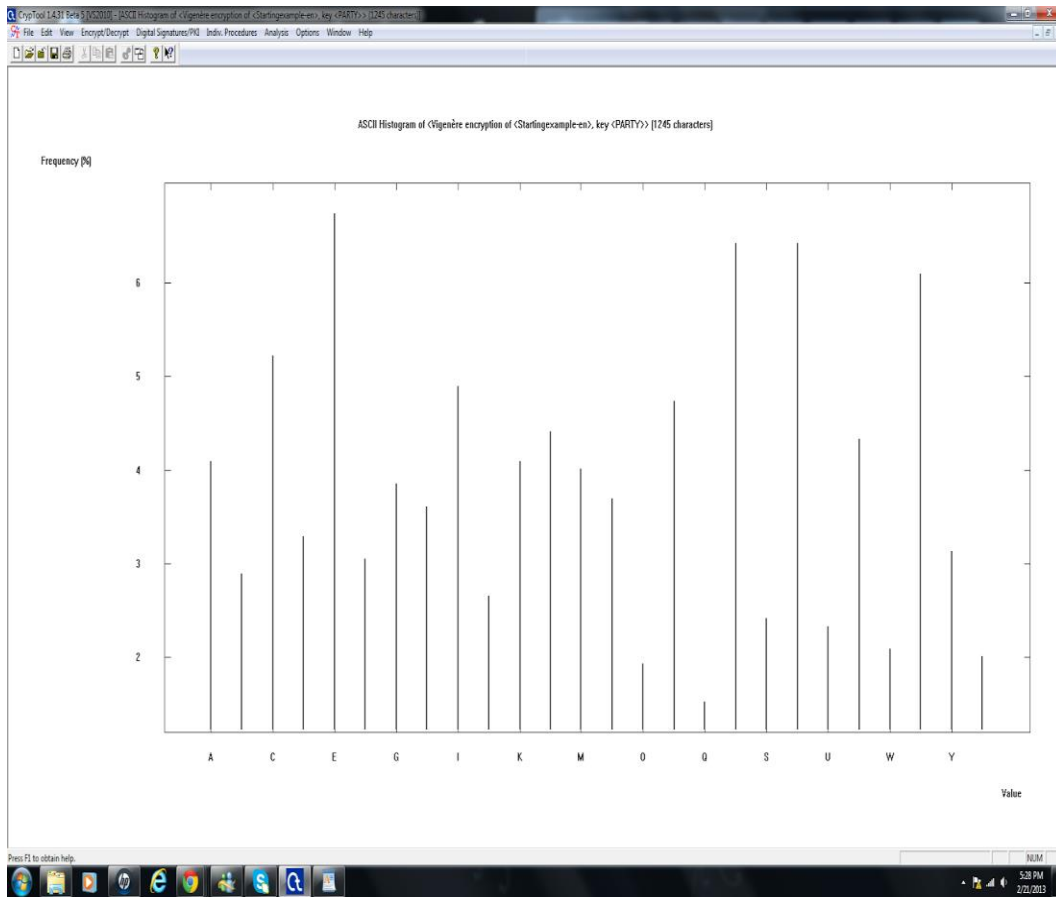
## AutoCorrelation

Property of



Histogram

Property of



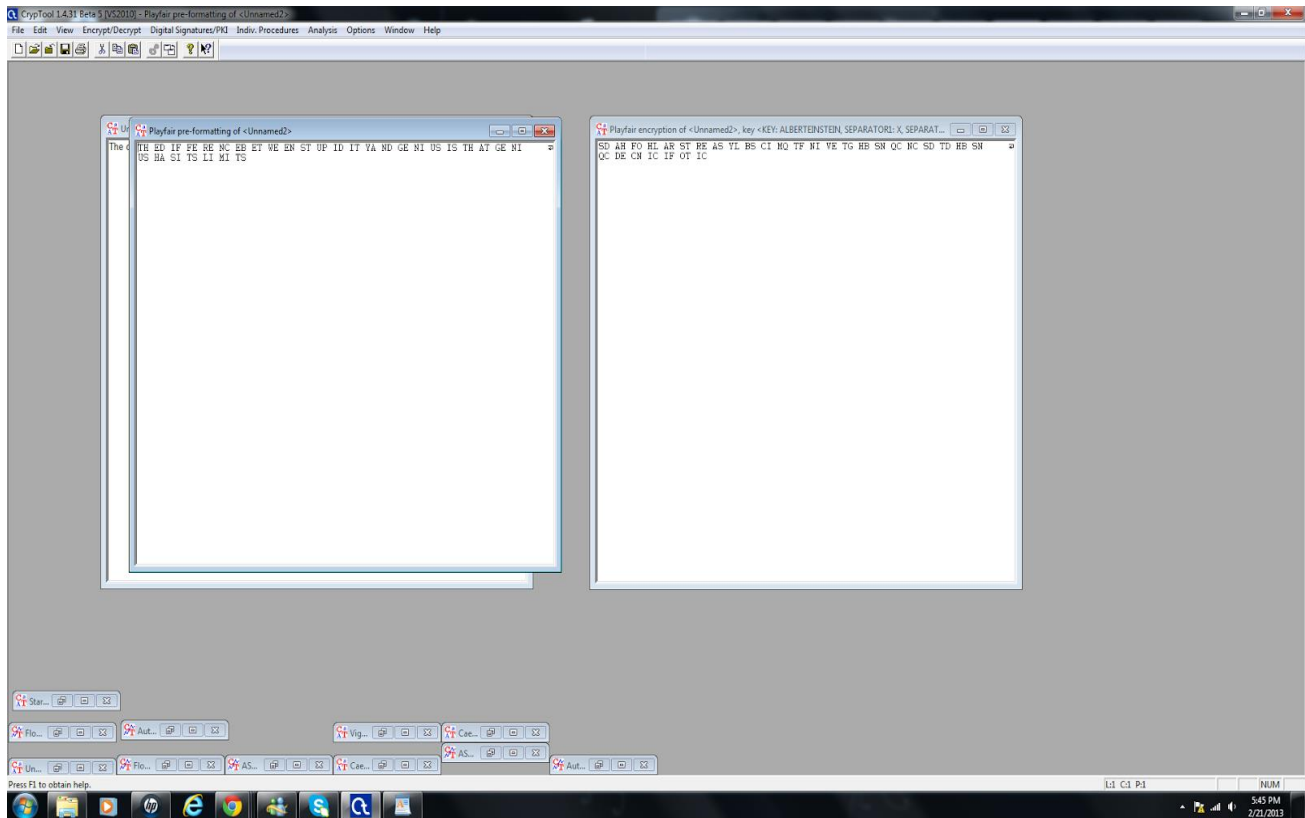
**Q2. What I noticed about the histogram results when text is encrypted with the Vigenère cipher in comparison to the results of the Caesar cipher and this is the case because:**

I notice that the text is harder to analyze the Vigenere because it is not just a shift of letters. There is not absolute pattern of letters and this makes it more complex. But the longer the pattern the easier it is to see the pattern of ciphertext which then it would be easy to encrypt. This was noticed long ago and was first published by "Friedrich Kasiski, a Prussian infantry officer [695]. He noticed that given a long enough piece of ciphertext, repeated patterns will appear at multiples of the keyword length." (Anderson, R., 2008). It is also more even in the frequency of the letters as to the Caesar Cipher having a higher frequency with just a few letters.

This is the case because it is a polyalphabetic substitution cipher that uses a series of Caesar Ciphers to encrypt the plaintext. This encrypts by using a keyphrase instead of just numbers.

*PLAYFAIR's Encryption*





Original (left) Encrypted(right)

**Q3. There is an error in the following ciphertext representation of this quote, what is it? What should the correct ciphertext be?**

**The original Encrypted message is:(THE CORRECT CIPHERTEXT)**

SD AH FO HL AR ST RE AS YL BS CI MQ TF NI VE TG HB SN QC NC SD TD HB SN QC DE CN IC IF OT IC

**The original un encrypted message is:**

TH ED IF FE RE NC EB ET WE EN ST UP ID IT YA ND GE NI US IS TH AT GE NI US HA SI TS LI MI TS

**This is the Error Example:**

SDAHFOWGRABSSRERIVBYBSCIMQTFNIVETGHBSNQCNCSDTDHBSNQCDECNICIFCTIC

**This is the decrypted quote of the Error example.:**

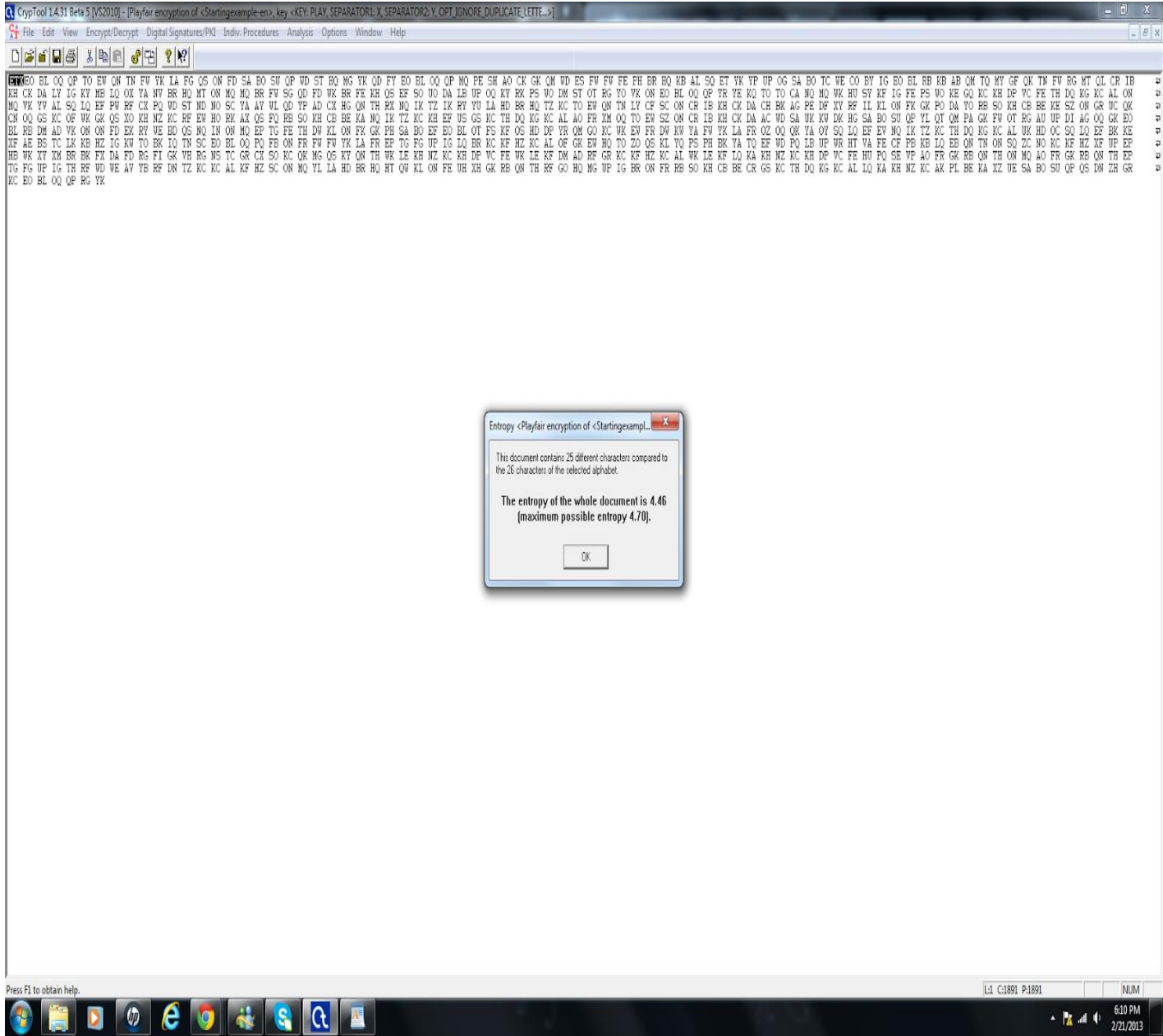
TH ED IF XF ER EN CE BE TW EX EN ST UP ID IT YA ND GE NI US IS TH AT GE NI US HA SI TS LI  
SC TS

We can see that the difference is that there are 2 letters inserted into the wrong one. There is an additional letter put in position 7 and 20. In the encrypted one it is displayed as an "X". I did this by putting in the encrypted message and then decrypting it using the passphrase. I then analyzed the information.

**Q4. Of the three ciphers discussed (Caesar, Vigenère, Playfair), the relative degrees of security and why are:**

These are the values decrypted in Playfair:

Property of Der Cyber



CrypTool 1.4.31 Beta 5 [V52010] - [Playfair encryption of «Startingexampl...» key «KEY\_SEPARATOR1: X, SEPARATOR2: Y, OPT\_IGNORE\_DUPLICATE\_LETTE...»]

File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

BE OQ OP TO EU ON TN FW YK LA FG OS ON FD SA BO SU QP HD ST HO NG YK QD FY EO BL OQ OP NO FE SH AO CK GK OM VD ES FV FW FE FH ER HO KB AL SO ET YK YP UP OS SA BO TC WE CO BY IG SO BL RB NB AB ON TO HT GF OK TW FV RG WT OL CR IB  
KA CK DA LY IG KY MB LQ OX YA NF BR HO NT ON NO MO BR FW SC QD FD WK BR FE HE OS EF SO NO DA LB UF OQ KY BK PS VO DM ST OT RS TO YK ON ED BL OQ YR YE KJ TO TO CA NO MO WK HU SF KF IG FE PS NO KE GQ KC KH DP VC FE TH DQ KS KC AL ON  
MO YK Y9 AL SQ LQ EF PF BK CK PQ UD ST ND NO SC YA AV VI QD YF AD CH HG ON TH RZ NO IX TZ IK PY YU LA HD BR HQ TZ KC TO EN ON TN LY CF SC ON CR IB KH CK DA CH BK AG PE DF ZY RF IL KL ON FW GK PO DA YO BE SO KH CB BE KE SZ ON GR UC OK  
CN OQ GS KC QP WK GK OS XO KH NZ KC PF EN HO BK AZ OS PQ RB SO KH CB BE YA NO IX TZ KC KH EF US GS KC TH DQ KG KC AL AO FW XM OQ TO EN SZ ON CR IB KH CK DA AC VD SA UK XW DW HG SA BO SU OQ YL OT OM PA GK FW OT BG AU UP DI AG OQ GK EO  
BL RE DH AD YK ON ON FD EK PY WE BO OS NO IN ON HO EP TG FE TH DW KL ON FX GK PH SA BO EF EO BL OT FS KF OS HD DP VR OM GO KC WK EW FR DW XW YA FW YK LA FR OZ OQ OX YA OY SO LQ EF EV NO IX TZ KC TH DQ KC AL UK HD OC SO LQ EF BK KE  
KF AE BS TC LK KB HZ IG KW TO BK IQ TH SC ED BL OQ PQ FB ON FR FW YK LA FR EP TG PG UP IG LO BR KC KF HZ KC AL OF GK EW NO TO ZO OS KL YO PS PH BK YA TO EF VD PQ LB UP UR HT VA FE CF PB KB LO EB ON TN ON SO ZC NO KC KF HZ XF UP EF  
HB WK XY XM BR BK FX DA FD RG FI GK VH RG NS TC GR CK SO KC OK MG OS KY ON TH WK LE KH NZ KC KH DP VC FE WK LE KF DM AD RF GR KC KF HZ KC AL UK LE KF LO KA KH NZ KC KH DP VC FE HU PO SE VP AO FR GK RB ON TH ON MO AO FR GK RB ON TH EF  
TG FG UP IG TH RF VD WE AV YB RF DN TZ KC KC AL KF HZ SC ON NO YL LA HD BR HQ HT OW KL ON FE VH XH GK RB ON TH RF GO HO MG UP IG BR ON FR RE SO KH CB BE CR GS KC TH DQ KG KC AL LO KA KH NZ KC AK PL BE KA XZ UE SA BO SU OQ OS DN ZH GR  
KC EO BL OQ QP RG YK

Entropy «Playfair encryption of «Startingexampl...»

This document contains 25 different characters compared to the 26 characters of the selected alphabet.

The entropy of the whole document is 4.46  
(maximum possible entropy 4.70).

OK

Press F1 to obtain help. L1 C:\891 P:\891 NUM 6:10 PM 2/21/2013

Caesar

Profi

The screenshot shows the Cryptool 1.4.31 Beta 5 interface. The main window displays text in a non-Latin script, likely a sample document used for encryption. A dialog box titled "Entropy <Caesar encryption of <StartingsampL..." is open in the center. The dialog box contains the following text:

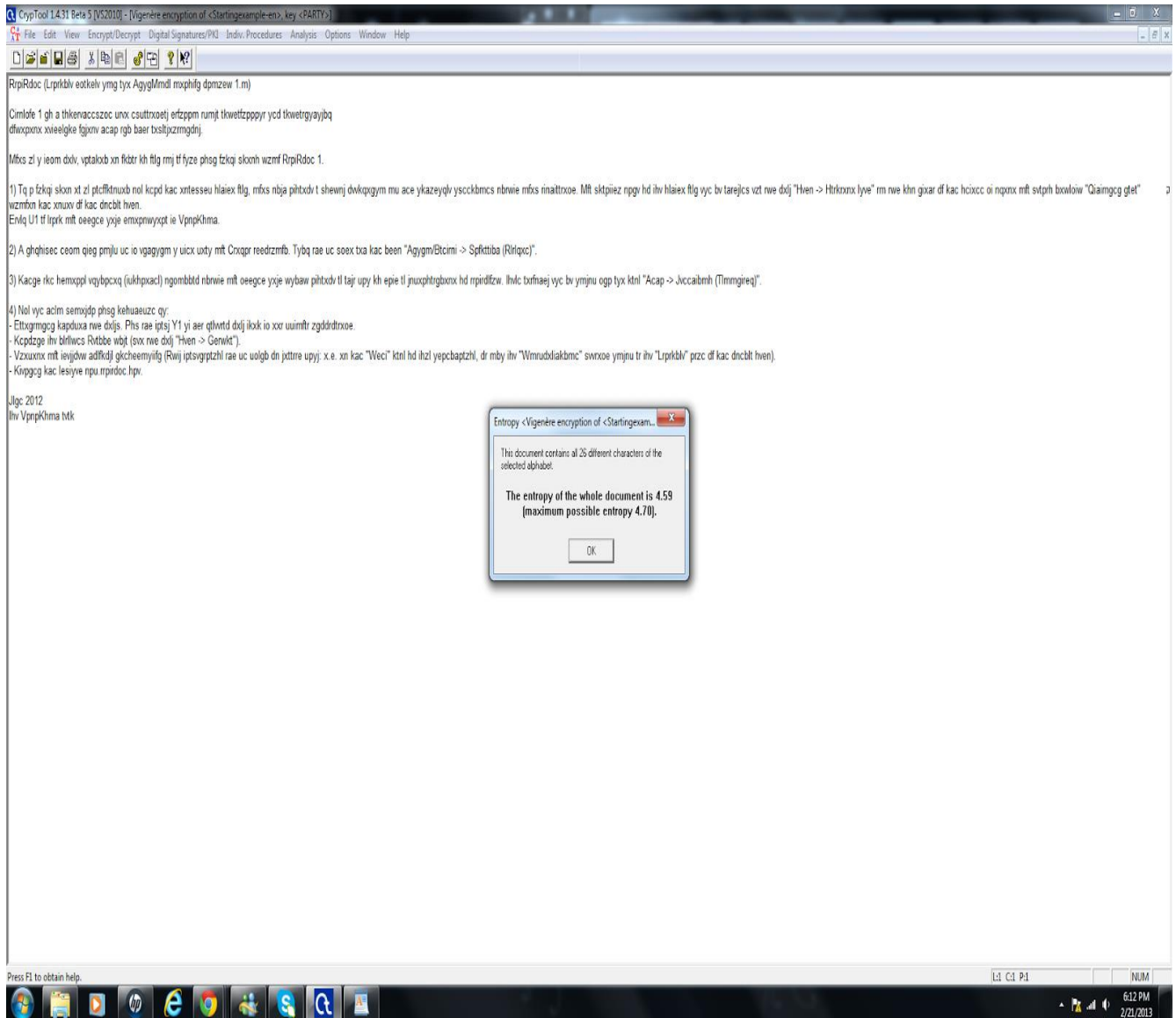
This document contains all 26 different characters of the selected alphabet.

**The entropy of the whole document is 4.18**  
(maximum possible entropy 4.70).

OK

The Windows taskbar at the bottom shows the system tray with the date 2/21/2013 and time 6:12 PM. The taskbar also includes icons for various applications and system utilities.

Vigenere



I was able to do an entropy test on the same cipher and this was the results of the test.

Caesar 4.18

Playfair 4.46

Vigenere 4.59

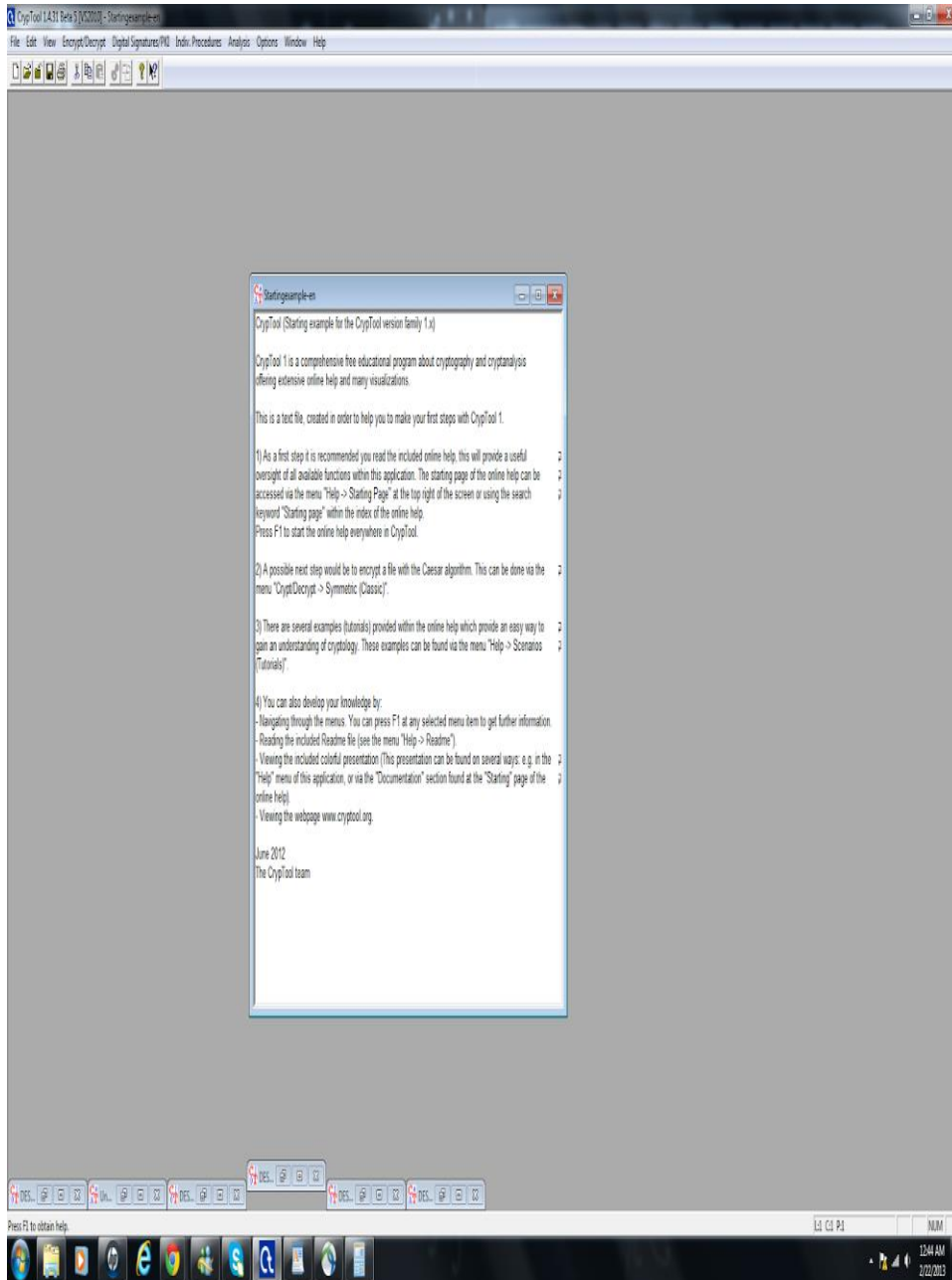
Max possible entropy is 4.70

This shows that the Vigenere has the highest degree of security.

the entropy tool is a tool that that measures the calculations of the occurrences of each character that is relative to each of the other ones.(CSEC 630 Lab Assignment 1 ) The higher that the value is calculated the less of a possibility that it will be able to be encrypted of deciphered.

## LAB 2

### Original Doc



DES(CBC) ENCRYPTION-LEFT / DECRYPTED DOC (with extra "NUL" on bottom) / DES(ECB)Encryption -right

The screenshot displays the Cryptool 1.431 Beta 5 interface. At the top, the title bar reads "Cryptool 1.431 Beta 5 [DES2010] - DES (ECB) decryption of <Startingexample-en>, key <00 00 00 00 00 00 00>, key <00 00 00 00 00 00 00 00>". The menu bar includes "File", "Edit", "View", "Encrypt/Decrypt", "Digital Signatures/PKI", "Indiv.Procedures", "Analysis", "Options", "Window", and "Help".

Three windows are open:

- DES (CBC) encryption of <DES (ECB) decryption of <Startingexample-en>, key <00 00 00 00 00 00 00 00>, key <00 00 00 00 00 00 00 00>:** Shows a hex dump of data. The first few lines are: 00000000 D1 33 DF 0D 5C 2C 94 21 D8 3A DF 0C 42 7E 06, 0000000F EE A1 7C B5 C8 96 CC A1 12 59 A1 E4 E5 11 0D, 0000001E B8 03 53 0E 19 B6 4C 31 F4 B0 07 94 2B B9 7C.
- DES (ECB) decryption of <DES (ECB) encryption of <Startingexample-en>, key <00 00 00 00 00 00 00 00>:** Displays the Cryptool 1.x help text. The text includes: "Cryptool (Starting example for the Cryptool version family 1.x)", "Cryptool 1 is a comprehensive free educational program about cryptography and cryptanalysis offering extensive online help and many visualizations.", "This is a text file, created in order to help you to make your first steps with Cryptool 1.", "1) As a first step it is recommended you read the included online help, this will provide a useful oversight of all available functions within this application. The starting page of the online help can be accessed via the menu 'Help -> Starting Page' at the top right of the screen or using the search keyword 'Starting page' within the index of the online help. Press F1 to start the online help everywhere in Cryptool.", "2) A possible next step would be to encrypt a file with the Caesar algorithm. This can be done via the menu 'Crypt/Decrypt -> Symmetric (Classic)'.", "3) There are several examples (tutorials) provided within the online help which provide an easy way to gain an understanding of cryptography. These examples can be found via the menu 'Help -> Scenarios (Tutorials)'.", "4) You can also develop your knowledge by: - Navigating through the menus. You can press F1 at any selected menu item to get further information. - Reading the included Readme file (see the menu 'Help -> Readme'). - Viewing the included colorful presentation (This presentation can be found on several ways: e.g. in the 'Help' menu of this application, or via the 'Documentation' section found at the 'Starting' page of the online help). - Viewing the webpage www.cryptool.org.
- DES (ECB) encryption of <Startingexample-en>, key <00 00 00 00 00 00 00 00>:** Shows a hex dump of data. The first few lines are: 00000000 D1 33 DF 0D 5C 2C 94 21 9D 9C C8 3A 92 C2 B8, 0000000F 28 24 6B C7 B4 C4 B4 2C 09 5C C0 93 08 8A 0F, 0000001E B6 65 2E 5F 30 14 6C E5 A0 13 03 74 F7 9E E2.

At the bottom of the interface, there is a taskbar with various icons and a system tray showing the date and time as 12:40 AM on 2/22/2013.

DES (ECB) - LEFT / PLAIN TEXT - MIDDLE / DES (CBC) - RIGHT





**a. an online bank statement**

This needs to use CBC because a bank's information needs to be more secure and the encryption needs to be more complex. CBC means Cipher Block Chaining and "Most commercial applications which encrypt more than one block use cipher block chaining" (Anderson, R., 2008). This mode is better for hiding patterns in plaintext.

**b. an encrypted VoIP session**

This needs to use ECB which stands for Electronic Code Book. ECB continues a general pattern and is less secure. In ECB you just encrypt block after block of plaintext to get the cipher. This works with VoIP because it is connectionless and does not need to be more secure.

**c. viewing of a website using TCP/IP**

This needs to use CBC because a website needs to be the most secure and TCP/IP sends out packets that are in order. This also dealing mainly with commercial applications would make a website most likely to use CBC.

Property of Der Cyber

## RSA 1

The screenshot shows the CrypTool 1.4.31 Beta 5 interface. A dialog box titled "RSA Demonstration" is open, showing the following parameters and results:

- Prime number p:** 59
- Prime number q:** 71
- Generate prime numbers:** (button)
- RSA modulus N:** 4189 (public)
- phi(N) = (p-1)(q-1):** 4080 (secret)
- Public key e:** 13
- Private key d:** 337
- Update parameters:** (button)
- RSA encryption using e / decryption using d (alphabet size: 256):**
  - Input as:**  test  numbers
  - Alphabet and number system options:** (button)
  - Input text:** test
  - The input text will be separated into segments of Size 1 (the symbol '#' is used as separator):** | # e # |
  - Numbers input in base 10 format:** 116 # 101 # 120 # 116
  - Encryption into ciphertext  $c[i] = m[i]^e \pmod{N}$ :** 0263 # 38793 # 4121 # 0953
- Buttons:** Encrypt, Decrypt, Close

The results with encrypting with numbers

$p = 59$

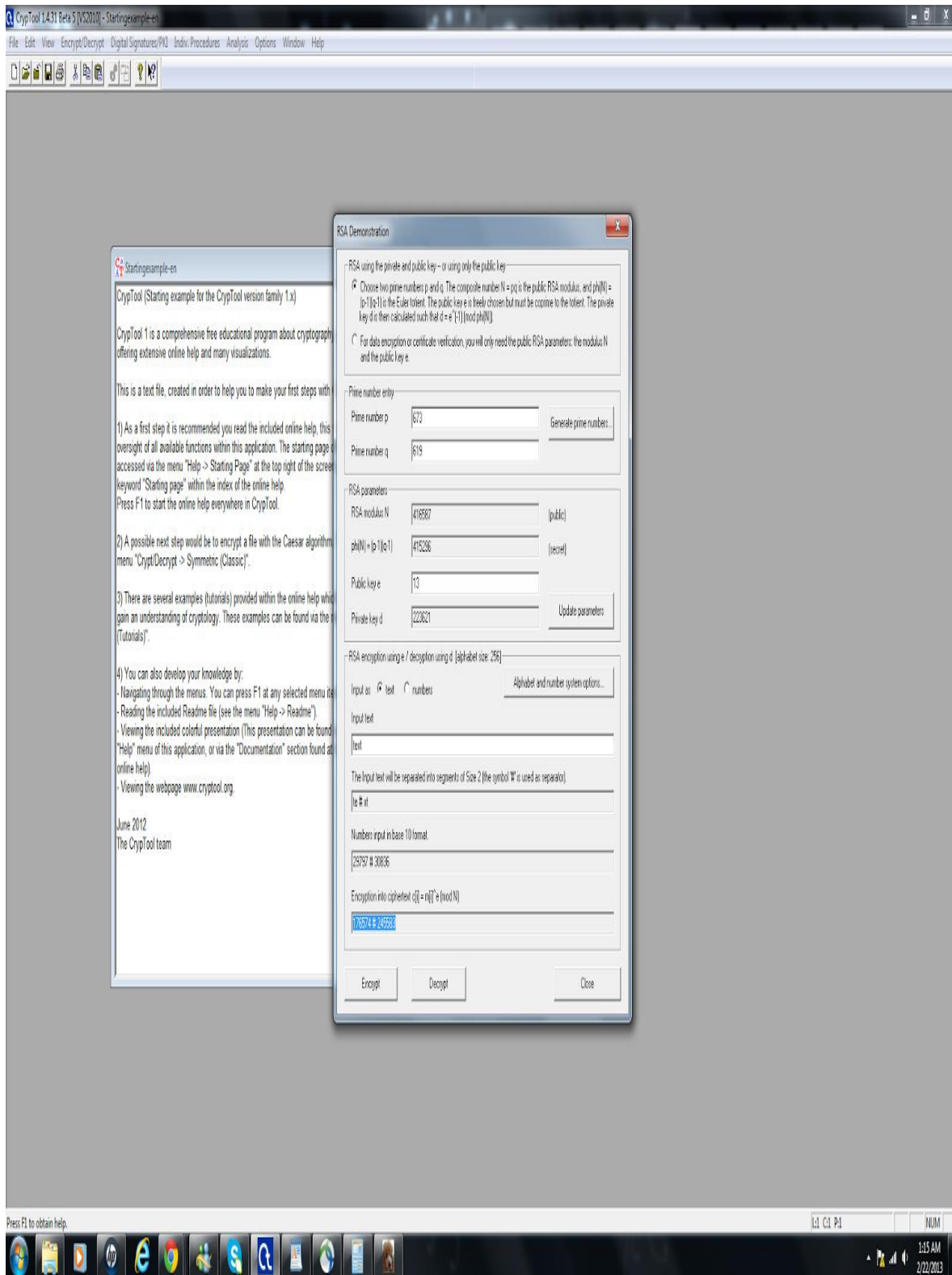
$q = 71$

$e = 13$

Encryption results are: 0953 # 3879 # 4121 # 0953

RSA 2

Property of Der Cyber



p = 673

$q = 619$

$e = 13$

Encryption results are : 176574 # 245583

**Q6. The difference I noticed in the block size, and whether or not this cipher would be susceptible to statistical analysis and why:**

What I notice about the block size is that it is dependent on the key that is inputted. So the longer or more complex the key is the longer the block size will be.

This would be susceptible to statistical analysis but the longer the key the harder it will be to compare. So it is possible to have a long key and the analysis be just about impossible and certainly improbable to carry out in a normal environment.

**RSA implementation**

**Q7. Analyze the data encrypted with the RSA cipher. How does this encryption method compare to the other methods the Lab has covered?**

The RSA uses an asymmetric encryption and this makes it more secure than the Symmetric encryption. Asymmetric uses a key for encryption and one for decryption while the other methods used symmetric encryption and this used one key for encryption and decryption. The longer the key is, the more secure and complex the cipher will be. This goes for both the symmetric and asymmetric encryption.

The con to RSA is that it takes up a lot more space/memory and will run slower. It needs more processing power and memory.

**Hybrid encryption**

# GUI Hybrid Encryption

CrypTool 1.431 Beta 5 [MS2010] - startingexample-en

File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

Hybrid Encryption with RSA-AES - Visualization with a Flow Chart

```

graph TD
    A[Open document] --> B[Document]
    C[Generate session key] --> D[Session key]
    E[Select asymmetr. key] --> F[Asymmetr. key]
    B --> G[Encrypt document symmetr.]
    D --> G
    D --> H[Encrypt session key asymmetr.]
    F --> H
    G --> I[Encrypted document]
    H --> J[Encrypted session key]
    I --> K[Save]
    J --> K
    L[Cancel]
  
```

startingexample-en

CrypTool (Starting example...)

CrypTool 1 is a comprehensive offering extensive online help...

This is a text file, created in...

1) As a first step it is recommended within this application. The screenshot the screen or using the search. Press F1 to start the online...

2) A possible next step would be "Symmetric (Classic)".

3) There are several examples...

startingexample-en

```

00000 43 72 79 70 54 6F 6C 20 28 53 74 61 72 74 69 6E 67 20 65  CrypTool (Starting e
00014 78 61 6D 70 6C 65 20 66 6F 72 20 74 68 65 20 43 72 79 70 54  xample for the CrypT
00028 6F 6F 6C 20 76 65 72 73 69 6E 20 66 61 6D 69 6C 79 20 31  ool version family 1
0003C 2E 78 29 0A 0A 0A 43 72 79 70 54 6F 6C 20 31 20 69 73  :x)....CrypTool 1 is
00050 20 61 20 63 6F 6D 70 72 65 68 65 6E 73 69 76 65 20 66 72 65  a comprehensive fre
00064 65 20 65 64 75 63 61 74 69 6F 6E 61 6C 20 70 72 6F 67 72 61  e educational progra
00078 6D 20 61 62 6F 75 74 20 63 72 79 70 74 6F 67 72 61 70 68 79  n about cryptography
  
```

Press F1 to obtain help.

l:l C:l P:l NUM

2:03 AM  
2/22/2013

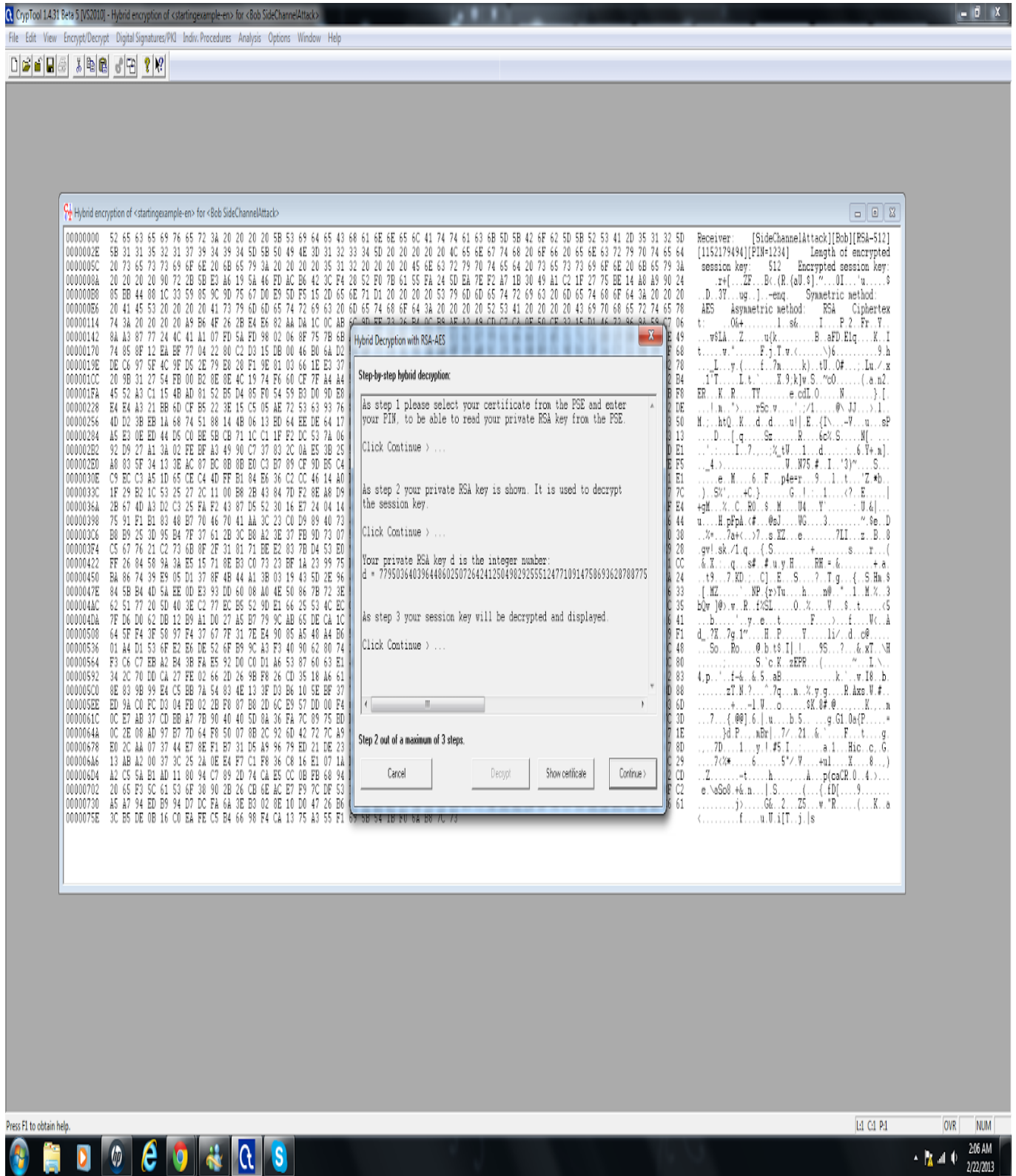


d =

7795036403964486025072642412504982925551247710914758693628788775938783545419  
3820408779009965640493205588280774002827039042768160696523493945630923917976  
57

Property of Der Cyber

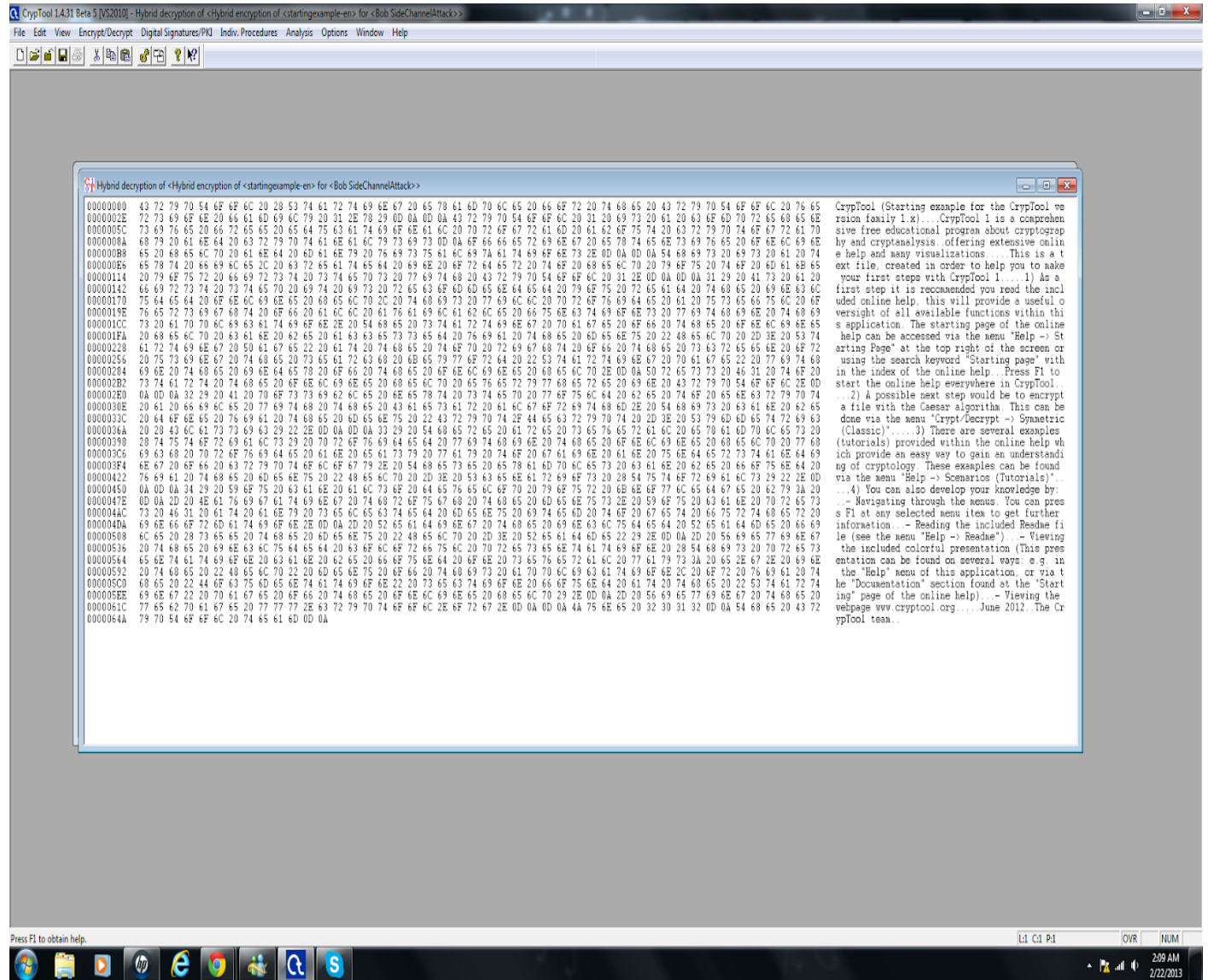




Then

The session key is the following 128 bit number:  
Session key: E9 06 B5 33 5F 59 1E 59 78 35 46 CB AF AE A2 E5

Then I Decrypted it and this is the Decrypted Doc:



HYBRID ENCRYPTION

The screenshot displays the Cryptool 1.431 Beta 5 interface. A window titled "Hybrid Encryption with RSA-AES - Visualization with a Flow Chart" is open, showing a process flow:

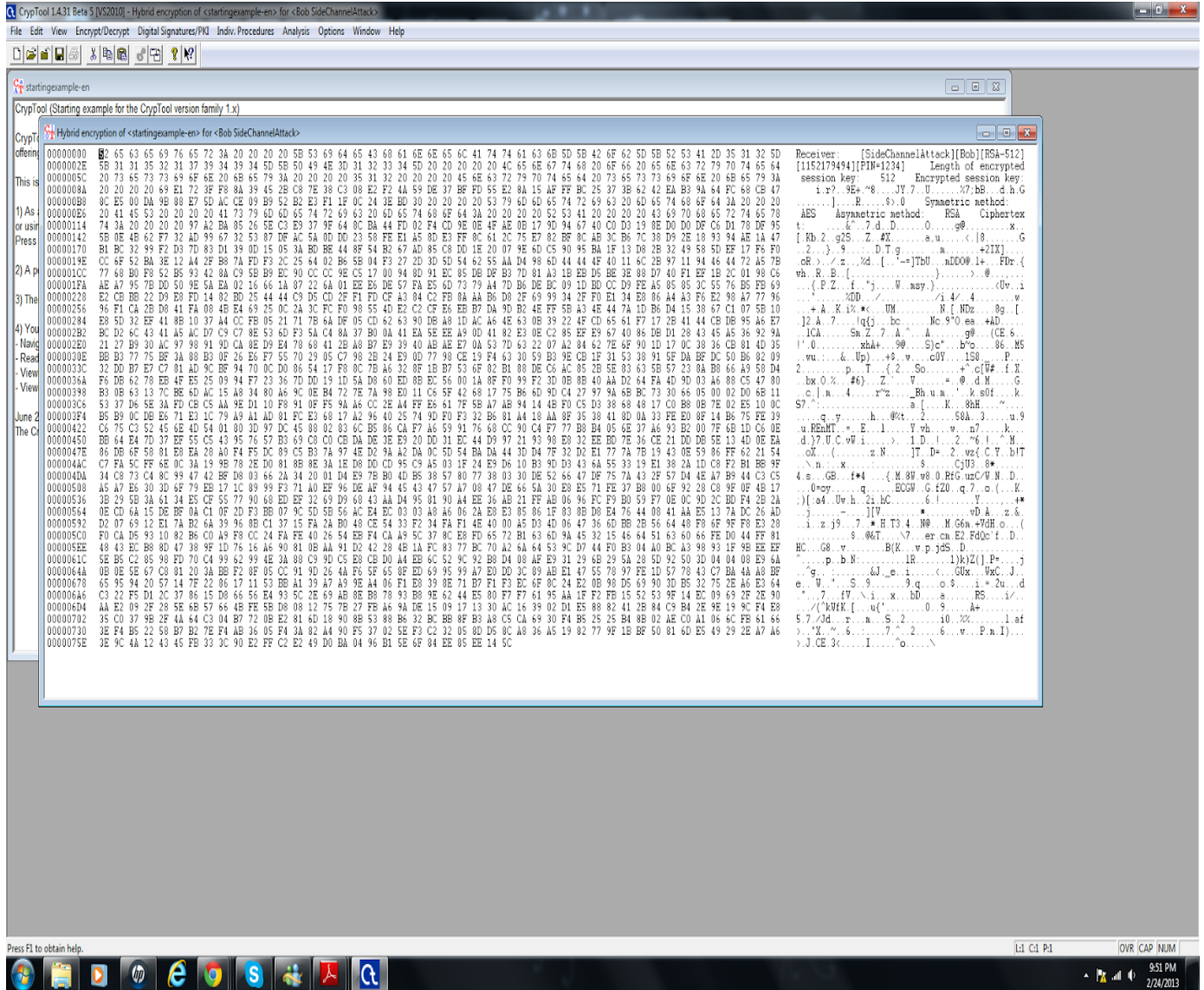
- Open document** (green hexagon) leads to **Document** (blue parallelogram).
- Generate session key** (green hexagon) leads to **Session key** (blue parallelogram).
- Select asymmetr. key** (green hexagon) leads to **Asymmetr. key** (blue parallelogram).
- Document** and **Session key** both lead to **Encrypt document symmetr.** (green rectangle).
- Session key** and **Asymmetr. key** both lead to **Encrypt session key asymmetr.** (green rectangle).
- Encrypt document symmetr.** leads to **Encrypted document** (blue parallelogram).
- Encrypt session key asymmetr.** leads to **Encrypted session key** (blue parallelogram).
- Both **Encrypted document** and **Encrypted session key** lead to a **Save** button (yellow oval).
- A **Cancel** button (yellow oval) is also present.

The background window shows the Cryptool main interface with a text file named "startingexample-en" open. The text includes instructions for using the software and a list of tasks:

- 1) As a first step it is recommended you read the included online help, this will provide a user manual or using the search keyword "Starting page" within the index of the online help. Press F1 to start the online help everywhere in Cryptool.
- 2) A possible next step would be to encrypt a file with the Caesar algorithm. This can be done in the menu "Encrypt/Decrypt" -> "Caesar".
- 3) There are several examples (tutorials) provided within the online help which provide an example of how to use the software.
- 4) You can also develop your knowledge by:
  - Navigating through the menus. You can press F1 at any selected menu item to get further information.
  - Reading the included Readme file (see the menu "Help->Readme").
  - Viewing the included colorful presentation (This presentation can be found on several ways in the menu "Help->Presentation").
  - Viewing the webpage [www.cryptool.org](http://www.cryptool.org).

June 2012  
The Cryptool team

## DATA Encryption of Hybrid Cipher



**Q8. The advantages of the Hybrid RSA-AES cipher and How does this encryption method compare to the other methods the Lab has covered are:**

Advantages of the Hybrid RSA-AES are many and one is that it still stays at the speed of symmetric encryption while protecting the data with the strength of asymmetric encryption. Because the symmetric encryption is about 100 % faster than asymmetric encryption this makes it more efficient and there are no sacrifices to security and the performance. This encryption uses the Pro's of each part of the encryptions.

This Encryption compares to the other methods in that they are either Symmetric or

Asymmetric. Symmetric is fast but not as secure and it needs to be known by both parties. Asymmetric is slow and only encrypts small amounts of data but is secure and only one party (the owner) of the Private key is able to encrypt and decrypt message from the public key. The Hybrid puts these both together and uses each. This is more secure and faster for equal symmetric processing.

#### Resources

CSEC 630 Lab Assignment 1 - Introduction to Cryptography

Anderson, R. (2008). Security engineering – A guide to building dependable distributed systems (2nd ed.). New York, NY: John Wiley & Sons Publishing, Inc. Chapter 5, "Cryptography"

Property of Der Cyber