**DATA ENCRYPTION**

**Activity 1:**

Cryptanalysis of the Vigen`ere Cipher The following ciphertext was encrypted using the Vigen`ere Cipher, where all spaces and punctuation were removed. Decrypt it, using any tool you like.

XUKW LGEE YINN WBVL BWKU VXUC XLQY FJSH NHNV PRCW GQRP GMAA SHTP VHIO TSJU IGJI JGFS QVFQ QRMM AFIE IEEV IAEV LRXB VSBN WNUC BWWR GWRX IECP BHXU GQNT INXE VNEO NINP HNTI DWMG GEON IGQT RTJB TQNH VRSY RPGL CRNN CFKW NPHG JYFV SRXI AIYR UWGJ IFGG EGXX GCBH XUKW PKTU GVCN ELKR TCVB WRQY MGJX UGQP CROG EYQX BHJH PFHV RBYT YGEF GJBT KRVE OQYG VLVU EAEM RPXF VYSH JBTX UGVR UXBH XUKW PQYE UIVP XUGV ROEV PHRT SSVL RESH TWRY IJKP YHSP WWBP QBTI RNEO QVNV ISQV ZUSS UIPW VVVC GJEG EEAP SGDI OTSX GROA WHEL NUMZ RPRV IPJR VSYR

**SOLUTION**

This year we also thought that you should at least once in your life browse the web for some kindergarten crypto tools as you see several of them are available and are quite able to perform a frequency analysis and thus to even guess the secret key of this cipher playing around with them can be a lot of fun but now please forget about this ancient stuff for the rest of this course in the remainder of the course we will focus on more elaborate forms of security that cannot be broken by such a simple technique.

The above Vigenere ciphertext was decrypted using the **Boxentriq** **tool** to generate its key because a ciphertext cannot be decrypted without a secret key. Here is a [link](https://www.boxentriq.com/code-breaking/vigenere-cipher) to the Boxentriq tool interface and a [video](https://vimeo.com/867110409/bc0adba41e?share=copy) showing the process of how the secret key was generated.

The secret key used is **ENC** and it was repeated multiple times to match the length of the ciphertext.

**Activity 2:**

Identify encryption schemes the task of this exercise is to find out which type of encryption was used for encrypting messages. The possible types are: Shift cipher (e.g., Caesar’s Cipher), Substitution Cipher and Vigenere. For each pair of plaintext and ciphertext find out which method of encryption was used and write down the key that was used for this method.

1. Plaintext: NEVER TRUST SECURITY BY OBSCURITY

Ciphertext: ARIREGEHFGVAFRPHEVGLOLBOFPHEVGL

1. Plaintext: THISISASECRETMESSAGE

Ciphertext: GSRHRHZHVXIVGNVHHZTV

1. Plaintext: GOOD

Ciphertext: OVUA

**A.** Plaintext: NEVERTRUSTINSECURITYBYOBSCURITY

Ciphertext: ARIREGEHFGVAFRPHEVGLOLBOFPHEVGL

**SOLUTION**

The type of encryption used here is the Caesar Shift Cipher using a ROT13.

The English Alphabet consists of 26 letters: A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z.

Now using the first letter N(from the plaintext above), N is in the position 14 in the alphabetical order written above, it will be encrypted by a shift of 13 or ROT13 which will arrive at A by counting forward to 13 i.e counting from 0(N),1(O), 2(P), 3(Q), 4(R), 5(S), to 13(A).

A shift key of **ROT13** was used in this process.

Below is a better explanation and definition of Shift and Caesar Cipher:

What is a Shift Cipher?

A shift cipher is a substitution cipher, the principle of which is to shift the letters by one or more values in the alphabet. A shift cipher encryption uses an alphabet and a key made up of one or more values that shifts the position of its letters.

A Caesar cipher is a shift cipher, it is a simple substitution cipher where the ciphertext alphabet is shifted a given number of spaces usually, presented with a shift key.

**B.** Plaintext: THISISASECRETMESSAGE

Ciphertext: GSRHRHZHVXIVGNVHHZTV

In this case, each letter of the ciphertext is shifted back by the corresponding letter in the keyword, using the Vigenère square. By reversing the process, the original plaintext message can be obtained.

The type of encryption used here is the **Reverse Cipher**.

Reverse Cipher uses a pattern of reversing the string of plain text to convert as cipher text. The process of encryption and decryption is the same. To decrypt cipher text, the user simply needs to reverse the cipher text to get the plain text.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| z | y | x | w | v | u | t | s | r | q | p | o | n | m | l | k | j | i | h | g | f | e | d | c | b | a |

**C.** Plaintext: GOOD

Ciphertext: OVUA

**SOLUTION**

The type of encryption used here is the **Vigenere Cipher**

**KEY: HGFW**