CRYPTOCACHE

Substitution Cipher

Substitution Cipher

To: Agent [redacted]
From: CONTROL

Hello agent,

The following coded message was intercepted by one of our field operatives. We know that the coded message contains the coordinates of a “dead drop” where an enemy agent will be passing information.

```
FYGXK ZVGRT UYOCT TOUIZ
RGZYG XKGFT LTCTF DOFWN
VTOUI ZTOUI ZRTUM TKGGF
TRGZM TKGFO FTMTK GFXSS
```

Your mission is to break the code and find the hidden “cache” containing the message between the enemy agent and his handlers.

This file contains the background material you will need to accomplish your mission.

Signed,

Control

Substitution Cipher

Background

The substitution cipher is one of the oldest ciphers on record. It dates back as far as the 4th century BC.

A substitution cipher is simply replacing every character in the "plaintext" (original message) with a specific other character or symbol to make up the "ciphertext" (secret message) for sending.

The Cryptocache Files contain several substitution ciphers, but this one is the most common and widely known.

You have probably seen this code in newspapers in the form of a "cryptogram" puzzle.

To create a crytogram-like substitution cipher, the first thing you need to do is determine the order of your "key" sequence.

For example, let's say you determine 'A' will replace 'R' in the ciphertext. You need to map out the other twenty-five letters with their replacements making sure each has a one to one pairing, meaning every letter is used once and only once.

Here is a sample key:

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
T	H	E	Q	U	I	C	K	B	R	O	W	N	F	X	J	M	P	D	V	L	A	Z	Y	G	S

The total number of possible keys (chosen at random) is:

26! (factorial)

or

26 x 25 x 24 x 23 ... x 2 x 1

or

403,291,461,127,000,000,000,000,000

While that seems like a lot of keys, modern computers can run through all those keys in less time than it took you to read this sentence.

Using the Code

The above key is not random. It was created by taking each of the letters in the phrase, “The quick brown fox jumped over the lazy dogs” and removing repeated characters as you go. Once you have created your key, you are ready to move on.

To encode a message you take every letter in your plaintext and find it in the top row of the key. You then replace it with the letter in the bottom row of the key.

So using this key, every ‘A’ becomes a ‘T’ and every ‘T’ becomes a ‘V’ and so on.

To decode the message, you do the reverse. You take each letter in the ciphertext and find it in the bottom row. You then replace it with the letter in the top row to get the decoded letter.

So using this key, every ‘T’ becomes an ‘A’ and every ‘A’ becomes a ‘V’ and so on.

Breaking The Code

The main trick to breaking a substitution cipher is to know the frequency of certain letters, meaning how common they are.

In the English language, the most common letter is ‘E’ so you might start by replacing the most common letter in the ciphertext with ‘E’ and see if any patterns appear.

In most common cryptograms you can also look for other patterns. You might start by replacing three letter words in the ciphertext with ‘AND’ or ‘THE’ and seeing if that helps with other words.

Unfortunately our spy is too clever for that. He is employing a common code trick of taking out all the spaces and then breaking the message up into blocks of five letters so you don’t know where each word starts and ends.

You do have another trick up your sleeve, though. It’s called a “crib.” A crib is a piece of text you know or believe to be in the original message. From there you start making up keys that decode blocks of text into your crib. If the same key starts making sense of the rest of the message, you are on the right track.

For example, we assume that this message contains coordinates for a secret location. If we can decode a block of text to be the word ‘EIGHT’ and that same key partially decodes a ‘TH*EE’ down the way, we can work out the remaining ‘R’ to help us with ‘ZERO’ and so on.

Good luck!