Royal Holloway University of London

Cyber Security Challenge UK

Puzzle III

One-Time Pad

The method used for this puzzle is a *one-time pad*, where each character of the plaintext is encrypted by a modular addition with a character of a secret key.

Providing that conditions are met (such as using a random key) this method is proven to be **unbreakable**! This is due to the range of potentially meaningful decodes messages obtained through cryptanalysis with different keys.

Thor and Captain America. (Marvel Comics, comicrelated.com, 2010)

Captain America and Thor use a one time pad to send each other messages. To do so they must share a **secret key** – to help them remember the **key** they used two words describing items they each own.

From our own analysis we have learned their **key** is 12 characters in length and begins with the letter "H". Can you guess their key and decipher the message?

Decode Instructions

To decode your ciphertext:

1. Align your repeating **key** to the **ciphertext** (repeat key if there is remaining ciphertext).
2. Take the first **ciphertext** value (e.g. $S = 18$ – use the lookup table).
3. Next take the first **key** value (e.g. $H = 7$ – use the lookup table).
4. Then take the **ciphertext** value plus the **key** value (e.g. $18 + 7 = 25$).
5. Finally, perform modulo 27. The modulus is 27 because that is the number of possible values. (e.g. $14 \mod 27 = 14$, which is `O`; $25 + 1 \mod 27 = 26$, which is `=`; or $26 + 1 \mod 27 = 0$, which is `A`). Modulus is like a 24-hour clock. The time after 23:58 is 23:59, 24:00 is written as 00:00, and 24:01 is written as 00:01; Modulo is just wrapping around a set value.
6. Repeat for each **ciphertext** character until finished!

0	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	=

Ciphertext

Decipher the following message:

Cipher	M	H	T	P	R	O	W	=	X	N	H	Y	K	E	Q	T	P	C	N	K
Key																				
Plain																				

Cipher	L	D	Q	K	M	H	T	Y	Q	B	B	B	V	A	A	B	U	G	I	T
Key																				
Plain																				

Your Answer