Royal Holloway University of London

Cyber Security Challenge UK

Puzzle V

Block Cipher (Electronic Code Book (ECB) Mode)

The method used for this puzzle is called a *block cipher, Electronic Code Book (ECB) mode*. Text is split up into fixed sided groups, or blocks, and transformations applied to each block individually.

There are a number of block ciphers and operating modes, each with distinct differences from others. ECB is the simplest mode where blocks are processed individually and errors are isolated to a single block, however identical plaintext blocks will produce identical ciphertext blocks aiding cryptanalysis efforts.

Dennis Nedry. (Jurassic Park, Universal Studios & Michael Crichton)

Oh no, it's Dennis, and he really knows his stuff! We'll never get the Park back online if you cannot solve this.

We know the **secret key** is 8 characters and am sure I saw him type the letter "`N`" somewhere.

Decoder

To decode your ciphertext:

1. Align your **key** to the **ciphertext** (repeat for the number of blocks).
2. Convert the **ciphertext** character decimal value to binary (use the lookup table).
3. Convert the **key** character decimal value to binary (use the lookup table).
4. XOR the binary **ciphertext** against the binary of the **key** (use truth table).
5. Convert the result from binary to decimal value, then find its **plaintext** character.
6. Repeat for each **ciphertext** character!

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	27	28	29	30	31
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	[	\	]	^	_	‘

Exclusive Or (XOR) work as follows:

A	B	Result
1	1	0
1	0	1
0	1	1
0	0	0

Binary numbers (base 2) work as follows:

16	8	4	2	1	Result	Binary	Character
0	0	0	0	1	1	1_2	A
0	0	1	0	0	4	100_2	D
0	1	0	0	1	9	1001_2	I
0	1	1	1	1	15	1111_2	P
1	1	0	1	0	26	11010_2	=

Ciphertext

```
\ G Z C S Y ‘ Z       J M B A D E [ U       N ] ] M V A ‘ [       H F L K A
```

Your Answer