Yellow Team

Security and Encryption are paramount here at JP Morgan chase & Co.

Without encryption and the use of authentication our customers would be highly vulnerable targets to malicious actors who would want to steal their personal information.

The challenge below shows how encryption and the use of keyed authentication can help to obfuscate information and to be sure that only those with the proper keys can view and use the protected data if it is received.

Part 1. Columnar Transposition

The key for the columnar transposition cipher is a keyword e.g. GERMAN. The row length that is used is the same as the length of the keyword. To encrypt a piece of text, e.g.

```
defend the east wall of the castle
```

we write it out in a special way in a number of rows (the keyword here is GERMAN):

G	E	R	M	A	N
d	e	f	e	n	d
t	h	e	e	a	s
t	w	a	l	l	o
f	t	h	e	c	a
s	t	l	e	x	x

In the above example, the plaintext has been padded so that it neatly fits in a rectangle. This is known as a regular columnar transposition. An irregular columnar transposition leaves these characters blank, though this makes decryption slightly more difficult. The columns are now reordered such that the letters in the key word are ordered alphabetically.

A	E	G	M	N	R
n	e	d	e	d	f
a	h	t	e	s	e
l	w	t	l	o	a
c	t	f	e	a	h
x	t	s	e	x	x

The ciphertext is created by going along the vertical columns. EX: nalcxeh…

Challenge: Use Columnar transposition with the keyword "Chase" to decrypt the message and retrieve the private key for part 2 Chase is spelled with the letters in alphabetical order.

Please use the provided scratch area for filling out the cipher table.

 **Note the "-" is a place holder and should be ignored in the final resulting alphabet key **

Padiz-mvnhjxeuwgc-lysbt-ofkrq-

Part 2. Caesar Cipher

To pass an encrypted message from one person to another, it is first necessary that both parties have the 'key' for the cipher, so that the sender may encrypt it and the receiver may decrypt it. For the caesar cipher, the key is the number of characters to shift the cipher alphabet.

Here is a quick example of the encryption and decryption steps involved with the caesar cipher. The text we will encrypt is 'defend the east wall of the castle' using the cipher alphabet.

```
plain:   abcdefghijklmnopqrstuvwxyz

cipher: bcdefghijklmnopqrstuvwxyza

plaintext:  defend the east wall of the castle

ciphertext: efgfoe uif fbtu xbmm pg uif dbtumf
```

Challenge: Use the answer from part 1 and overlay the alphabet below with your generated alphabet from part 1.

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

Encoded Message :   rdfse mko rmc pamre

Yellow Team

Part 1 Answer:

A	C	E	H	S

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

Part 2 Answer:

_____