Khudeja Begum

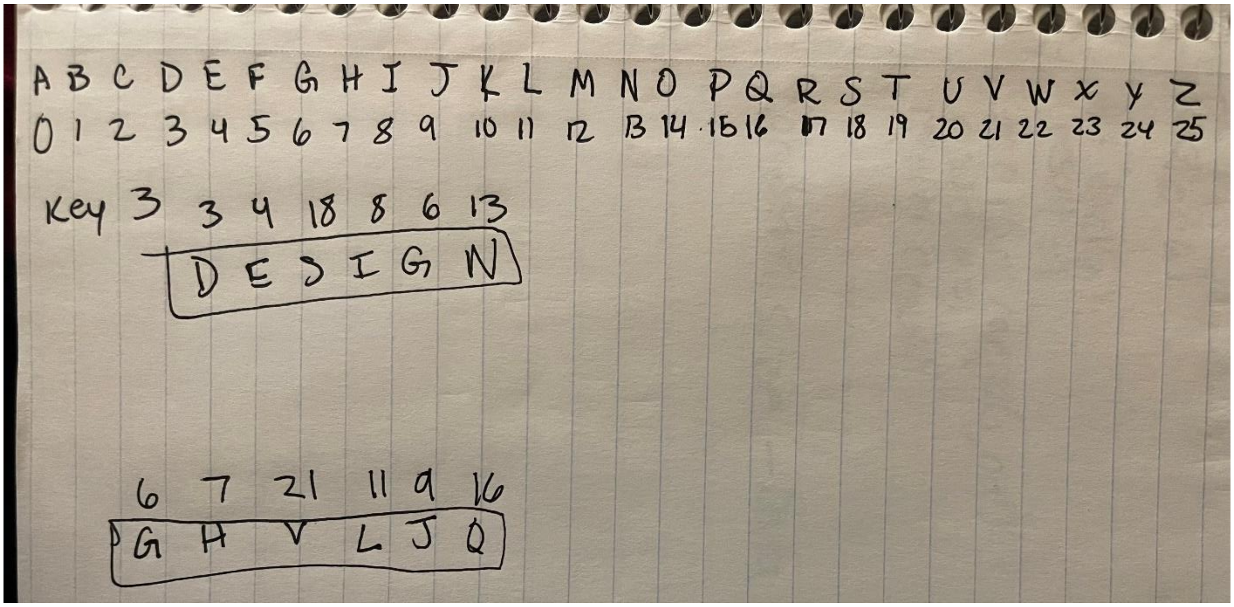
No collaboration

Extension: No

Sources: stackflow & google

Due: 7/20/22

Part 0



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
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

Key 3 3 4 18 8 6 13

D E S I G N

6 7 21 11 9 16

G H V L J Q

Extra Credit:

2) A one-time password (OTP) is **an automatically generated numeric or alphanumeric string of characters that authenticates a user for a single transaction or login session**. An OTP is more secure than a static password, especially a user-created password, which can be weak and/or reused across multiple accounts. The use of one-time password tokens **hardens a traditional ID and password system by adding another, dynamic credential**. Depending upon the vendor, an OTP token will generate a PIN synchronously or asynchronously. Synchronous tokens use a secret key and time to create a one-time password.

3) Security tokens can fail or break. Process of OTP password generation can be cumbersome. If an attacker can mount a known plaintext attack, he can get part of your keystream and decrypt anything that was encrypted using this part of the keystream.

4) OTP attack SMS-based One-Time Passwords (SMS OTP) were introduced to counter phishing and other attacks against Internet services such as online banking. Today, SMS OTPs are commonly used for authentication and authorization for many different applications.