One Time Pad - encryption using modular arithmetic*

* and importantly! with key as long as message whose are elements random

This article about one-time pads gives examples of using modular arithmetic in cryptography.

Part 1 - alphabetic encryption using modulo 26 arithmetic

Please read the article's sections entitled "About Modular Arithmetic" and "Is One-time pad Unbreakable?". It says:

> "The modulus should have the same value as the number of different elements that need to be calculated, with 0 designated to the first element. Thus, for bits (0 or 1) we use modulo 2 and for bytes...we use modulo 256 .... For digits (0 through 9) we use modulo 10.... Performing modulo calculations on letters..., we must assign the values 0 through 25 to the letters A through Z and then use modulo 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
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

It gives this example of an alphabetic encipherment (see its paragraph entitled "Is One-time pad Unbreakable?"):

plaintext		T	O	D	A	Y
OTP-key	+	X	V	H	E	U
	-------------------					
ciphertext		Q	J	K	E	S

Example: Q is derived from T and X by modulo 26 addition. T being 19 and X being 23, T+X is 19+23=42 but modulo 26 addition says we take not the sum itself but the remainder from dividing that sum by 26, which is 16. Hence, Q. Same for the other 4 letters.

What if instead of "TODAY" we want to encrypt "HELLO" and we choose the key "JFZTE"? What is the ciphertext?

Suppose we want to encrypt "APPLE" and we'd like to get the same ciphertext as when encrypting "TODAY" above? What key would it take to accomplish that?
And if we want to encrypt "GLASS" and get that same ciphertext, what key accomplishes it?
And if we want to encrypt "READY" and get that same ciphertext, what key accomplishes it?

And if we want to encrypt "MONTH" and get that same ciphertext, what key accomplishes it?

So the matching plaintext for ciphertext "QJKES" is "GLASS". And, the matching plaintext for ciphertext "QJKES" is "READY". And also "MONTH". All correct. Also THING, COLOR, HEART, PUREE, VALUE, SPICE, BRING, EXTRA, STRAW, and many others. Apparently, all 5-letter words in English (or not even in English, but all 5-letter combinations whatsoever) *are* correct plain text for ciphertext "QJKES".

Part 2 - number encryption using modulo 10 arithmetic

This is another way to encrypt alphabetic letters. It too involves a letter-to-number conversion step, but a different one. After the letters are represented by numbers, those numbers are subjected to encryption using some chosen one-time key.

Please read the article's sections entitled "One-time Pad with Numbers" and "A Practical Example with Numbers".

The letter-to-number conversion system this time uses the following "straddling checkerboard":

		0	1	2	3	4	5	6	7	8	9
	|	A	T		O	N	E		S	I	R
2	|	B	C	D	F	G	H	J	K	L	M
6	|	P	Q	U	V	W	X	Y	Z	.	fig

Its purpose is economy, achieved by representing the most frequent symbols in the language with only one digit, consuming two of them only for less frequent symbols. The letters in the top row are English's frequent ones. Any of those gets representation by the single digit above it. So T is 1, I is 8. No letter gets 2 nor 6. Those are reserved for use as the first of a 2-digit representation for the other letters. In examining text ciphered this way, if you see a 2 or 6 it does not correspond to any letter. Rather, you must marry it to the number that follows to compose a 2-digit code and that one gives you a letter. If you see any of the other 8 digits, you have its letter.

The exercise to perform

Listen to this short-wave radio broadcast from a numbers station, which reaches you as a special agent behind enemy lines. It contains a message which, by one-time pad pre-arrangement, you know to have been encoded by subtraction with the following key:

```
66153 77185 10800 54937 48159 83271 12892 07132 34987 53954 23074
```

The radio is broadcasting a ciphered message to you. It is to be figured out with the above key. You have that key printed on the pad you smuggled in when you penetrated enemy territory. Since the coding used subtraction, you will need to apply (carryless) addition to decode. You'll add the broadcast ciphertext together with the above key. The numbers that emerge will be the plaintext represented through the above straddling checkerboard. When you tune in to receive your coded message, ignore the call sign that occupies the broadcast's first 1 minute 22 seconds. The message starts at that point with "66475" and continues thereafter. Write it down, apply the key to it, and refer the resulting numbers to the checkerboard to get letters. That will yield the plaintext and enable you to answer questions 7-9 below. Note that while Part 1 used modulo 26 arithmetic to treat the numbers that represented letters, here we use modulo 10 arithmetic to do the same thing by applying carryless addition and borrowless subtraction (which *is* modulo 10 arithmetic).

Answer the following questions:

1. The ciphertext resulting from encrypting HELLO with key JFZTE modulo 26 is:

a. YDXWJ
b. KOSZU
c. QJKES
d. AEGCB
e. FPQVT

2. The key that encrypts APPLE modulo 26 to yield ciphertext QJKES is:

a. MHPKZ
b. DCBYW
c. AFELQ
d. OGTNI
e. QUVTO

3. The key that encrypts GLASS modulo 26 to yield ciphertext QJKES is:

a. KYKMA
b. ZHPLE
c. UYSQW
d. JAXIT
e. XJURV

4. The key that encrypts READY modulo 26 to yield ciphertext QJKES is:

a. NHWC

b. ZKSGD
c. VOCND
d. ZFKBU
e. BKMGR

5. The key that encrypts MONTH modulo 26 to yield ciphertext QJKES is:

a. QYLEJ
b. EVXLL
c. FVOAT
d. IMXUR
e. PTNWG

6. Can a brute force attacker who stole your "QJKES" ciphertext, upon trying key "JFZTE" and discovering that "HELLO" emerges, correctly conclude that he has determined your plaintext to be "HELLO"?

a. yes
b. no

7. The topic of the numbers station message broadcast to you is:

a. weapons
b. a national leader
c. a town
d. travel schedules
e. documents

8. The action that the message instructs you to take is to:

a. report
b. change
c. kill
d. deliver
e. destroy

9. The timeframe for you to take that action is:

a. tomorrow
b. midnight
c. two weeks
d. 21:00
e. 3 days