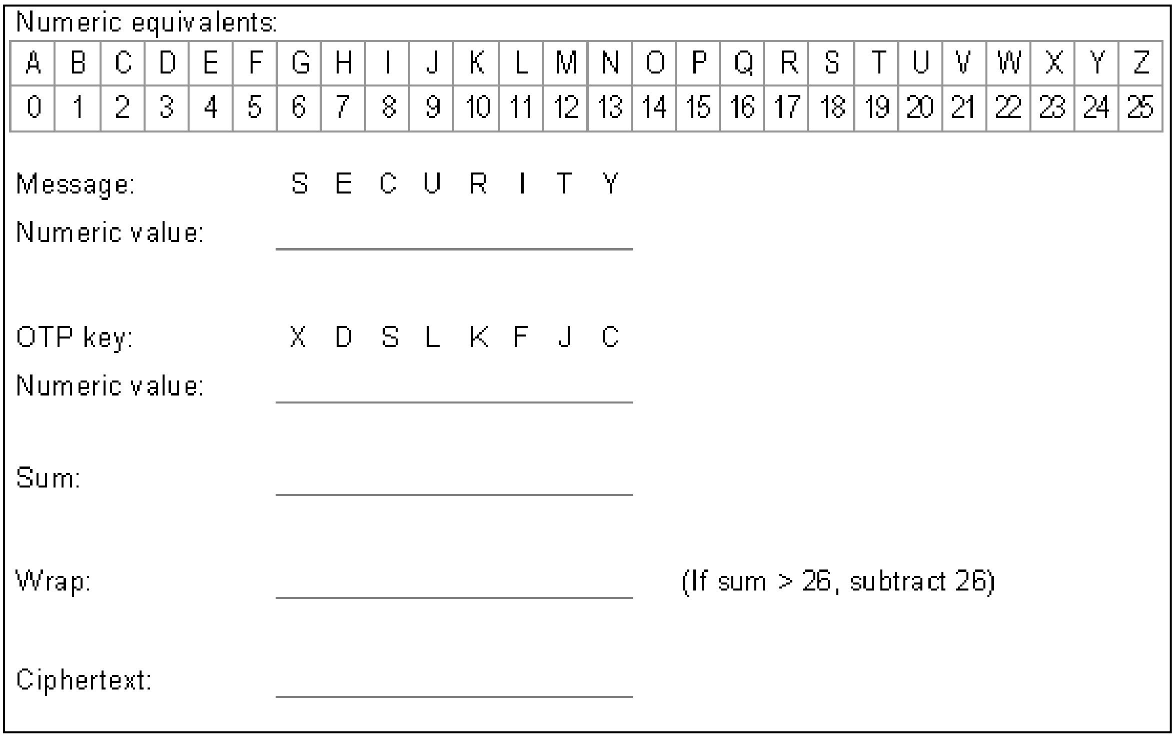
Encrypting and decrypting data with a one-time pad

Worksheet



Numeric equivalents:

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

Message: S E C U R I T Y

Numeric value: ____________________

OTP key: X D S L K F J C

Numeric value: ____________________

Sum: ____________________

Wrap: ____________________ (If sum > 26, subtract 26)

Ciphertext: ____________________

Here's how	Here's why
1. Your mission is to encrypt a message and transmit it securely to your partner, using the one-time pad worksheet above.	
2. Find the numeric equivalent for each letter in the message.	You can write your answers in the space provided within the exhibit.
1. Find the numeric equivalent for each letter in the OTP key.	As with all one-time pad keys, it's the same length as the message and consists of randomly generated letters.
2. Add the numeric equivalents for the message's letters to the values for the OTP, and write the sum in the Sum line.	
5. If the sum is less than 26, write the value on the Wrap line. For any sums greater than or equal to 26, subtract 26 and then write that value on the Wrap line.	

6. Find the letter equivalents for each of the numbers you calculated, and write them on the Ciphertext line.	This is the encrypted message you’d transmit to your partner.
3. If you were really using this one-time pad to send an encrypted message, what should your next step be?	
4. Time to switch roles: You’re now the recipient of the ciphertext, and your mission is to decrypt the message.	Because this is a symmetric cipher, the decryption message uses the same key. In this case, the decryption algorithm is essentially the inverse of the encryption algorithm. You would have received the OTP key earlier, through a secure means of transmission.
5. Find the numeric equivalents for each of the letters in the ciphertext.	
6**.** From those numbers, subtract the numeric equivalents for the corresponding character in the OTP key.	You can use the values you computed earlier. Some values will be negative.
10. To each numeric value, add 26.	
11. If the result is over 26, subtract 26.	
12. Find the letter equivalents for each of the numbers you calculated.	This is the decrypted message, which should match the original text.