ONE-TIME PAD METHOD

One-Time Pad encryption is a multi-layered process that uses random numbers to encrypt a message. The Soviets (as well as other countries) routinely used the One -Time Pad method from WWII into the beginning of the Cold War. Some entities may still be using use this system. The elegance of this encryption technique is obvious. If necessary, encryption could be done entirely by hand, and if done properly the encryption is believed to be uncracking able even with today's supercomputers.

Encryption low

$$C = (P + K) \bmod 26$$

Decryption low

$$P = (C - K) \bmod 26$$

The one-time pad offers complete security but, in practice, has two fundamental difficulties:

1. There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.
2. Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

Example 1

Encrypt the message "Communication" if the following key is (9 20 13 0 21 1 13 19 9 5 25 12 25 4 7 25 0 8 8 7 24 2 6 18 16 10 23 5 11 12 13 6 22 22 17 3 8 0 0 19 4 15)

Answer

Encryption process

C = (P + K) mod 26

Paintext	C	O	M	M	U	N	I	C	A	T	I	O	N
	2	14	12	12	20	13	8	2	0	19	8	14	13
Key	9	20	13	0	21	1	13	19	9	5	25	12	25
Add	11	34	25	12	41	14	21	21	9	24	33	26	38
Mod 26	11	8	25	12	15	14	21	21	9	24	7	0	12
Cipher	L	I	Z	M	P	O	V	V	J	Y	H	A	M

Decryption process

In decryption process, We want to find the plain text

P = (C - K) mod 26

Cipher	L	I	Z	M	P	O	V	V	J	Y	H	A	M
	11	8	25	12	15	14	21	21	9	24	7	0	12
Key	9	20	13	0	21	1	13	19	9	5	25	12	25
sub	2	-12	12	12	-6	13	8	2	0	19	-18	-12	-13
Mod 26	2	14	12	12	20	13	8	2	0	19	8	14	13
Paintext	C	O	M	M	U	N	I	C	A	T	I	O	N

Example 2

Encrypt the plaintext "Fourth year" and the key is multipliers of three that less than 26

Answer

Encryption process

C = (P + K) mod 26

Paintext	F	O	U	R	T	H	Y	E	A	R
	5	14	20	17	19	7	24	4	0	17
Key	3	6	9	12	15	18	21	24	3	6
Add	8	20	29	29	34	25	45	28	3	23
Mod 26	8	20	3	3	8	25	19	2	3	23
Cipher	I	U	D	D	I	Z	T	C	D	X

Decryption process

P = (C - K) mod 26

Cipher	I	U	D	D	I	Z	T	C	D	X
	8	20	3	4	8	25	19	2	3	23
Key	3	6	9	12	15	18	21	24	3	6
Sub	5	14	-6	-8	-7	7	-2	-22	0	17
Mod 26	5	14	20	18	19	7	24	4	0	17
Paintext	F	O	U	R	T	H	Y	E	A	R