

1. Terminology

encryption

decryption

plaintext

ciphertext

key

2. **Shift cipher:** Each letter in the message is shifted a fixed number of steps over.

For example, below we use a shift of 3: $A \rightarrow D$, $B \rightarrow E$, ...

	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
plain	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
cipher	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

(a) Encrypt the plaintext **E N T R Y**

(b) Suppose the following text has been encrypted with a shift cipher using the shift $A \rightarrow D$ (a shift of 3). Decrypt it.

T X R W H