Vigenère Cipher

Overview

A substitution cipher replaces the characters in a message but does not rearrange them.

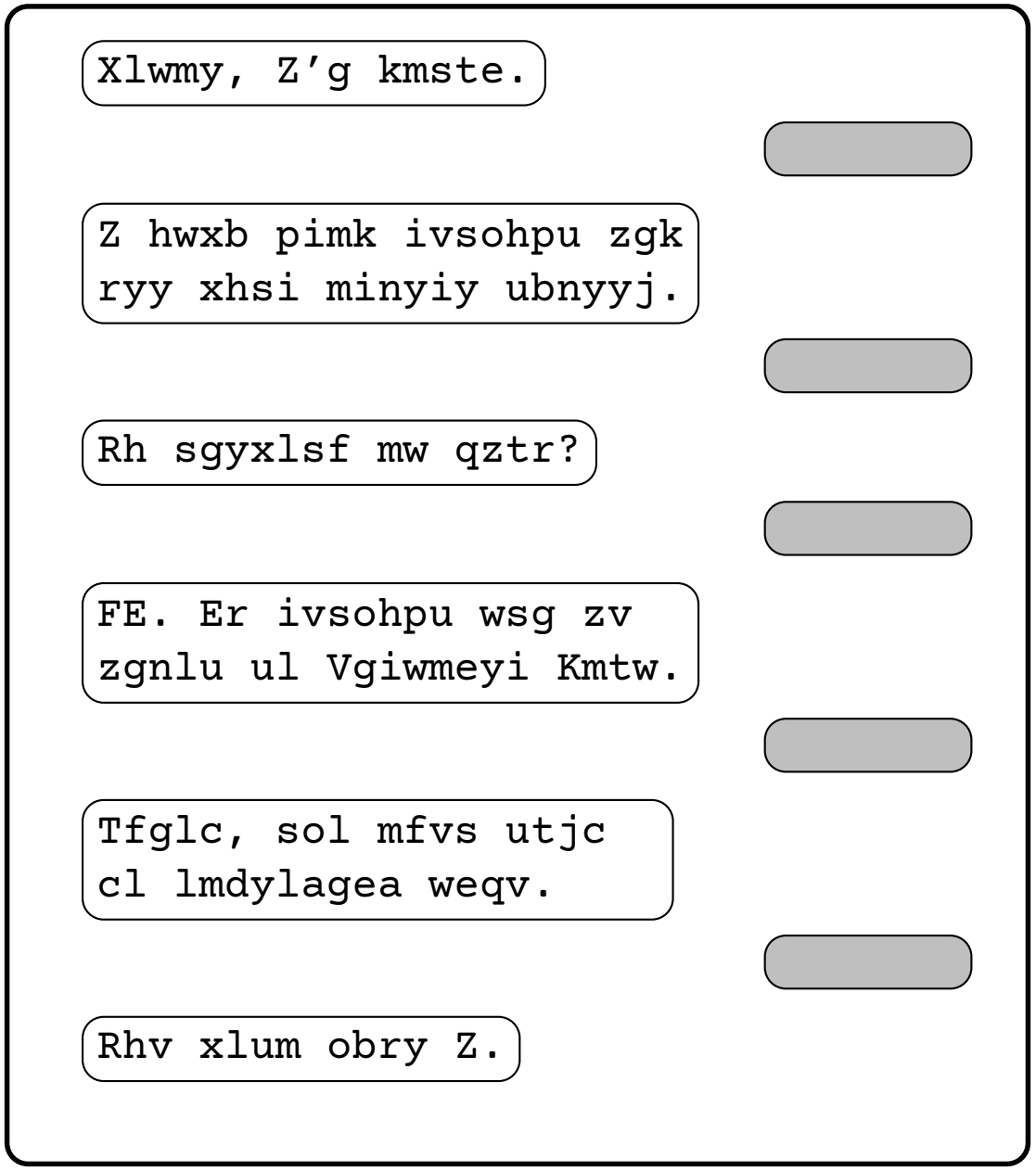
A polyalphabetic substitution cipher is a cipher that uses more than one substitution alphabet.

The Vigenére cipher is a famous polyalphabetic substitution cipher. The substitution alphabets are determined by a secret keyword agreed upon ahead of time by the message's sender and receiver.

Encryption

To encrypt a message of length ℓ with a keyword:

1. Write out the keyword, repeating as necessary to create a key of length ℓ.
2. For each character in the key, compute the distance in the alphabet between that character and the letter A.
3. Shift each character of the message forward by the distance computed for its position in step 2.



Example

Use the keyword DEADBEEF to encrypt the message:

A LONG TIME AGO

1. Write out the keyword, repeating as necessary to create a key of length $\ell = 12$.

Message:	ALONGTIMEAGO
Key:	DEADBEEFDEAD

2. For each character in the key, compute the distance between that character and the letter A.

D	E	A	D	B	E	E	F
3	4	0	3	1	4	4	5

3. Shift each character in the message forward by the amount computed in the previous step.

Message:	ALONGTIMEAGO
Key:	DEADBEEFDEAD
Shift:	340314453403

After restoring the spacing from the original message, this yields the ciphertext:

D POQH XMRH EGR