CodeCrackers Instruction Manual

Substitution Cipher Study Guide

A substitution cipher replaces each letter in the alphabet with a unique counterpart. Unlike the Caesar cipher, where the shift is consistent, substitution ciphers use a custom, randomized mapping of the alphabet. This makes them more resistant to brute-force attacks, but they can still be cracked with frequency analysis and pattern recognition.

How It Works

1. Create a 1-to-1 mapping between each letter of the alphabet and a substitute letter.
2. Every time a letter appears in the plaintext, replace it with its mapped substitute.
3. Decryption uses the reverse mapping to reconstruct the original message.

Example Mapping:
A -> Q, B -> M, C -> Z, D -> S, E -> V, ...

Encryption Example

```
Mapping    : H->D, E->V, L->C, O->P
Plaintext : HELLO
Ciphertext: DVCCP
```

Decryption Example

```
Mapping     : D->H, V->E, C->L, P->O
Ciphertext  : DVCCP
Decrypted   : HELLO
```

Practice Problems

Using the following mapping:
A->Q, B->M, C->Z, D->S, E->V

```
1. Encrypt: BEAD
2. Decrypt: TWRT (Assume matching reverse mapping)
3. Encrypt: BACK
4. Encrypt your own message using the above map
```

Answers

```
1. BEAD   -> MVSQ
2. TWRT   -> BACK
3. BACK   -> MQZE
```

CodeCrackers Instruction Manual

Crack the Cipher Challenge

Ciphertext: VQLL ZQ VU HCFZH

Hint: The most common letter in English is 'E'.

Use letter frequency and pattern analysis to break the code.

Study Tips

- Repeated letters (like LL) may hint at common double letters like EE or LL.

- Look for short words: 1-letter words are likely A or I, 3-letter words might be THE.

- Make a frequency chart if you're working with long messages.

- Substitution is case-insensitive by default, but spacing and punctuation usually stay untouched.

- Try building your own cipher maps and trading messages with friends to practice.