UNIVERSITI TEKNOLOGI MARA

Reverse Frequency Cipher

CSC662 – COMPUTER SECURITY

DR. FERAS ZEN ALDEN

2021435138 – Muhammad Zulkifli Bin Mohd Zin

2021288136 – Muhammad Adam Fitri Bin Abd Rani

2021223204 – Mohamad Nur Syazwan Bin Mohd Noor

2022234426 – Khairul Syahmi Bin Azman

Main Focus

Reverse Frequency Cipher

A custom encryption method where:

- Most frequent letters → least common ones
- Unique map per message
- Optional Caesar cipher makes it more secure

Step 1: Clean Input

```
const clean = text
  .toUpperCase()
  .replace(/[^A-Z]/g, '');
```

- Remove punctuation
- Keep only A-Z
- Case-insensitive

Step 2: Count Frequencies

```
const freq = {};
for (const ch of clean) {
  freq[ch] = (freq[ch] || 0) + 1;
}
```

- Track how often each letter appears

Step 3: Sort by Frequency

```
const sorted = Object.keys(freq).sort((a, b) =>
  freq[b] - freq[a] || a.localeCompare(b)
);
```

- Highest frequency → first
- Alphabetical tie-break

Step 4: Generate Map

```
const reversed = 'ETAOINSHRDLCUMWFGYPBVKJXQZ'.split('').reverse();
const map = Object.fromEntries(
  sorted.map((ch, i) => [ch, reversed[i]])
);
```

- Least-used English letters become most-used in your result
- Makes it unpredictable

Step 5: Apply Map

```
const cipherMap = reverse
  ? Object.fromEntries(Object.entries(map).map(([k, v]) => [v, k]))
  : map;
```

- For **decryption**, map is flipped
- Keeps encryption/decryption in sync

Making It Secure

Hybrid with Caesar Cipher

To meet security rubric, we combine:

- 🔁 Reverse frequency mapping
- ➕ Optional Caesar cipher rotation
- 🔒 Double encryption layer

Caesar Shift (Snippet)

```
function shiftChar(char, n) {
  const base = char === char.toLowerCase() ? 'a' : 'A';
  return String.fromCharCode(
    ((char.charCodeAt(0) - base.charCodeAt(0) + n + 26) % 26) + base.charCodeAt(0)
  );
}
```

- Rotates letters
- Supports wrap-around
- Works for both cases

Apply Caesar in Hybrid

```
let finalChar = useCaesar
  ? shiftChar(subChar, shift)
  : subChar;
```

- Caesar shift is optional
- Adds randomness to the mapped output

Why Combine?

Layer	Purpose
Frequency Map	Unique cipher
Caesar Cipher	Added security
Combined Logic	Harder to crack

Strengths

- Unique cipher based on input text
- Less predictable than fixed substitution
- Easy to implement and understand
- Optional Caesar adds extra security

Limitations

- Still vulnerable to frequency analysis (if text is long)
- Repeated characters may reveal patterns
- No secret key involved — map is predictable if text is known

Summary

- 🔐 Message-based cipher map
- 🔁 Optional Caesar cipher
- 📌 Decryption requires both text & saved map
- ✅ Meets secure encryption criteria

Demo

Thank You

Questions?