PART 2

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

The logic behind is a simple substitution, where each letter of the alphabet is replaced by another specific letter. The letters on the left side of the list represent the original alphabet, and the letters on the right side represent the corresponding encoded letters.

By way of example, the first three letters of the alphabet are shifted three spaces to the right, so A - B - C corresponds to D - E - F. Subsequently, D - E - F shift three spots to the left, and correspond to the letters A - B - C. So, A = D, B = E, C = F, D = A, E = B, and F = C. This is applied to the rest of the letters in the alphabet, until you reach the letters Y and Z, which are swapped.

PlainText: I LOVE CRYPTOGRAPHY!
ENCIPHER: LIRSB FOZMWRJODMKZ$

DECIPHER: I LOVE CRYPTOGRAPHY

PART 3

July 2019 marked one of the most notable data breaches in recent history, targeting Capital One Financial Corporation. This breach compromised the personal information of millions of customers and highlighted the need for enhanced cybersecurity measures across the industry.

The Capital One data breach involved the unauthorized access and theft of personal and financial information of approximately 106 million individuals in the United States and Canada. The alleged perpetrator, Paige A. Thompson, a former employee of Amazon Web Service, was arrested and charged with various computer fraud and abuse offenses.

The motivations behind the breach were primarily financial gain and data theft. By compromising Capital One's systems, the perpetrator aimed to obtain sensitive personal information, including names, addresses, credit scores, social security numbers, and bank account details. Such information can be exploited for various purposes, such as identity theft, fraudulent financial activities, or sold on the dark web for profit.

The breach at Capital One was primarily facilitated by vulnerabilities stemming from technical flaws in their infrastructure. The primary weakness was attributed to a misconfiguration in the company's cloud-based servers hosted on the Amazon Web Services (AWS) platform. The misconfiguration allowed the perpetrator to exploit a server-side request forgery (SSRF) vulnerability. This flaw enabled unauthorized access to the sensitive data housed in the cloud environment.

Paige Thompson discovered the vulnerability by scanning the internet for misconfigured servers. By exploiting the SSRF vulnerability, she gained unauthorized access to a server's metadata service, which in turn provided access to Capital One's systems. Thompson then exfiltrated the data from the compromised servers and stored it on her own servers and GitHub repositories.

Since the data breach, Capital One took several steps to enhance its security measures and protect against similar vulnerabilities.

1. **Configuration Management Process:** The company reinforced its configuration management processes, ensuring proper and secure configurations for their cloud-based servers. Regular audits and security assessments are conducted to identify and rectify any misconfigurations promptly.
2. **Stricter Access Controls:** They also implemented stricter access controls and permissions management to prevent unauthorized access to sensitive data. Multi-factor authentication (MFA) and role-based access control (RBAC) mechanisms were strengthened to mitigate the risk of unauthorized access.
3. **Threat Detection and IDS:** The bank bolstered its threat detection capabilities through the deployment of advanced security tools and technologies. This includes intrusion detection systems (IDS), security information and event management (SIEM) systems, and continuous monitoring to identify and respond to potential security incidents promptly.
4. **External Consultants:** Capital One also engaged external cybersecurity experts and conducted comprehensive security assessments to identify potential vulnerabilities and develop effective

countermeasures. By seeking external expertise, the company aimed to gain a broader perspective on security practices and ensure a more robust defense posture.

The Capital One data breach was one of the most serious in recent history and teaches us that even large corporations can be susceptible to cyber attacks.