**PART 2**

**KEY**

A-Z

B-Y

C-X

D-W

E-V

F-U

G-T

H-S

I-R

J-Q

K-P

L-O

M-N

N-M

O-L

P-K

Q-J

R-I

S-H

T-G

U-F

V-E

W-D

X-C

Y-B

Z-A

!-.

**ENCIPHERED PHRASE**

I love cryptography!

R OLEV XIBKGLTIZKSB.

The first part, from A to Z, shows a mapping of each letter in the alphabet to another letter to form a key. For example, A is being replaced by Z, B by Y, C by X, and so on, until Z is replaced by A.

Using this substitution key, we can decipher the encoded phrase "R OLEV XIBKGLTIZKSB" by reversing the substitution process.

Deciphering each character accordingly, we obtain the original phrase: "I love cryptography!"

**PART 3**

1. **Research major cybersecurity breaches over the past 20 years and pick one to write a short essay on.**

In July 2017, Equifax, one of the largest credit reporting agencies in the United States, made an announcement that hackers had successfully breached Equifax's systems, compromising the personal information of approximately 147 million individuals. This breach was a stark reminder of the vulnerabilities in our digital infrastructure and the pressing need for robust cybersecurity measures.

The Equifax data breach exposed a wealth of sensitive information, including names, social security numbers, birth dates, addresses, and even driver's license numbers. The sheer magnitude of the breach made it one of the most significant cybersecurity incidents in recent history. The compromised data provided cybercriminals with the tools to engage in identity theft, fraudulent activities, and financial exploitation.

“ [In September of 2017, Equifax announced a data breach that exposed the personal information of 147 million people. The company has agreed to a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories. The settlement includes up to $425 million to help people affected by the data breach. “

1. **Give an overview of what the breach was and the motivations behind it.**

Cybercriminals often target large organizations like Equifax because they possess vast amounts of valuable personal information. In this case, the stolen data could be exploited for various malicious purposes, such as identity theft, financial fraud, and even targeted phishing attacks

1. **Explain where the “tech flaws” were, and how hackers were able to breach their system.**

Hackers exploited a software vulnerability in Apache Struts, gaining unauthorized access to Equifax's network. Equifax's security mechanisms failed to detect the breach, allowing the hackers to operate undetected for an extended period. The incident highlighted the importance of timely patching, robust network security, and effective incident response in mitigating such breaches.

1. **What has the company done to protect against that vulnerability since?**

Equifax prioritized timely patching and vulnerability management, strengthened network security through enhanced segmentation and access controls, and improved incident detection and response capabilities. They also focused on employee training and awareness, engaged in external auditing and compliance assessments, and implemented stronger encryption and data protection protocols

**Source:**

https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement