Part 2

Logic: To send out a hidden message disguised as gibberish to then be translated back into words.

Phrase: “I love cryptography!”

Private Cipher:

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

* Phrase after
  + C SGYD QMKVOGZMRVTK!

Public Cipher:

| S | Y | K | Q | V | Z | R | M |
| --- | --- | --- | --- | --- | --- | --- | --- |
| L | V | Y | C | P | G | A | R |

* Phrase after
  + \_ L\_V\_ CRYP\_\_G\_A\_\_Y
  + \_ LOVE CRYP\_OG\_A\_\_Y
  + I LOVE CRYPTOGRAPHY

Part 3

I decided to do some research on the Colonial Pipeline hack that happened in May of 2021. The breach was done by a group named DarkSide. They targeted the pipeline’s digital systems with a ransomware attack, causing it to shut down for several days. Within a two hour window, the attackers stole 100 gigabytes of data, and left the system infected affecting billing and account systems.

The hackers were able to gain access by an exposed password for a VPN account. The password from an employee was used in another location which had a data breach, in turn causing this VPN to no longer be secure.

Since the attack, the company has implemented SBOM, Software Bill of Materials. This SBOM allows the builder to make sure components are up to date and respond quickly to any new vulnerabilities that rise up.