Part 2:

My cipher will have the following 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

“I love cryptography!” = “R olev xibkgltizksb!”

Part 3:

Linkedin Breach Number 1

In June of 2012, LinkedIn experienced a cyber breach where a hacker stole 6.5 million unassociated passwords. With the stolen data, the hacker was then able to log into these accounts scrape email addresses and passwords of those users and eventually put that data up on the market (a Russian Hacker Forum) for just 5 bitcoins. A cybersecurity student at UC Berkely explained how the hacker was able to steal the passwords:

“The hacker found a LinkedIn employee who happened to also self-host his website. While there was nothing of interest on that site for the hacker, he also found a different site being hosted on the same server. A WordPress site.

Now, most people in tech know WordPress is terribly vulerable to exploits. The hacker knew this too, and uploaded a malicious PHP script (essentially using SQL injection), which granted him admin access to the server where the site was being hosted.

Poking around the server, the hacker found it was actually a VM… running on an iMac. The employee’s personal iMac. The hacker was able to hop from the VM onto the iMac, and from there, the hacker found an RSA key, which granted him access to LinkedIn. Boom. He was in.”

So in this case LinkedIn’s tech flaws was the lack of precaution from one employee. However, there is still blame on LinkedIn because the hacker had access to data but still had to crack the individual passwords of the users. This is were everything goes to sh!t. Linkedin was using SHA-1 hashing for their passwords, which were unsalted, so there was no randomness to the hash. This made those passwords vulnerable and more hackable. Thus, 6.5 million accounts were hacked and the data which the accounts held was sold on a secondary market.

Since 2012 the company has updated password hashing with salting and asked users to setup dual authentication. By taking precautions on both the user and server ends, Linkedin has been able to avoid other catastrophic data breachs.