Vincenzo D'Aria

CS 492 HW #1

#1 A) 2^{64} → # of Keys to brute force in 64 bit encryption.

2^{45} → # of keys machines can crack per second

So, $2^{64-45} = 2^{19} = 524288$ seconds

$= \frac{524288 \text{ sec}}{31,536,000 \text{ sec/year}} \approx \boxed{.0167 \text{ years}}$

B) 2^{128} → # of possible keys to brute force in 128-bit encryption

2^{45} → # of keys machnes can crack per second

So, $2^{128-45} = 2^{83} \approx 9.67 \times 10^{24}$ seconds

$= \frac{9.67 \times 10^{24} \text{ Seconds}}{31,536,000 \text{ sec/year}} \approx \boxed{3.067 \times 10^{17} \text{ years}}$

#2

#2 Plaintext = Crypto to hide data

$$\begin{array}{cc} & \begin{array}{cccc}1&2&3&4\end{array}\\ \begin{array}{c}1\\2\\3\\4\end{array} & \begin{bmatrix}c&r&y&p\\t&o&t&o\\h&i&d&e\\d&a&t&a\end{bmatrix}\end{array} \xrightarrow{(2,1,4,3)} \begin{array}{cc} & \begin{array}{cccc}1&2&3&4\end{array}\\ \begin{array}{c}2\\1\\4\\3\end{array} & \begin{bmatrix}t&o&t&o\\c&r&y&p\\d&a&t&a\\h&i&d&e\end{bmatrix}\end{array}$$

$$\xrightarrow{(3,4,4,2)} \begin{array}{cc} & \begin{array}{cccc}3&4&1&2\end{array}\\ \begin{array}{c}2\\1\\4\\3\end{array} & \begin{bmatrix}t&o&t&o\\y&p&c&r\\t&a&d&a\\d&e&h&i\end{bmatrix}\end{array} \rightarrow \boxed{C = \text{totoypcrtadadehi}}$$

So, the resulting cyphertext: