

Travis Takushi 11791772

1. continued

Security: $\Pr[M=m | C=c] = \Pr[M=m]$

Explanation: enc is $C=(m+k) \bmod n$, every possible m and every possible c , there is exactly one k which satisfies the equation, which is uniformly generated

\therefore all ciphertexts are equally likely regardless of m

$\therefore \Sigma_n$ is perfectly secure

$\therefore \Sigma^*$ is perfectly secure because every two letter string maps to exactly one number in \mathbb{Z}_{676} and every number in \mathbb{Z}_{676} maps to exactly one two letter string

Black box means you don't know the process only the input and output. The major advantage is that it makes the encryption perfectly secure a lot more easily because you aren't creating keys or schemes in a way that biases to how the blackbox works, as well as you don't need to worry about how it works for it to work

2. Find any message $m = (m_1, m_2) \in \mathbb{Z}_n \times \mathbb{Z}_n$ and any ciphertext $c = (c_1, c_2) \in \mathbb{Z}_n \times \mathbb{Z}_n$. Solve for the key $k = (k_1, k_2)$ satisfying $C = \text{Enc}_k(m)$

$$C_1 = (m_1 + k_1) \bmod n \Rightarrow k_1 = (c_1 - m_1) \bmod n$$

$$C_2 = (m_2 + k_2) \bmod n \Rightarrow k_2 = (c_2 - m_2) \bmod n$$

\therefore there is exactly one key that produces c from m , $k = (c_1 - m_1 \bmod n, c_2 - m_2 \bmod n)$

Keys are uniformly sampled from $\mathbb{Z}_n \times \mathbb{Z}_n$

$$\therefore \Pr[\text{Enc}_k(m) = c] = \Pr[k = k] = \frac{1}{n^2}$$

$$\therefore \Pr[C = c | M = m] = \Pr[C = c | M = m'] \therefore \Pr[M = m | C = c] = \Pr[M = m] \text{ for all } m, c$$

$$\text{Dec: } \text{Dec}_{(k_1, k_2)}(c_1, c_2) = ((c_1 - k_1) \bmod n, (c_2 - k_2) \bmod n)$$

$$\text{if } c_1 = (m_1 + k_1) \bmod n, \text{ then } m_1 = (c_1 - k_1) \bmod n$$

$$c_2 = (m_2 + k_2) \bmod n, \text{ then } m_2 = (c_2 - k_2) \bmod n$$

3. Find any message $m = m \in \mathbb{Z}_n$ and any ciphertext $c = c \in \mathbb{Z}_n$, solve for the key $k = (k_1, k_2)$ satisfying $\text{Enc}_k(m) = c$, look at set of keys for m to encrypt c
~~or find m, k such that $m \cdot k_1 + k_2 = c \pmod n$~~
 $S_{m,c} = \{(k_1, k_2) \in \mathbb{Z}_n \times \mathbb{Z}_n : m \cdot k_1 + k_2 \equiv c \pmod n\}$
 for any fixed choice of $k_1 \in \mathbb{Z}_n$ there is exactly 1 k_2 solving $m \cdot k_1 + k_2 \equiv c \pmod n$
 $k_2 \equiv c - m \cdot k_1 \pmod n$

$\therefore |S_{m,c}| = n$ because there is only one matching pair for each uniquely encoded k_1 and k_2 .

$$\therefore \Pr[C=c | M=m] = \frac{|S_{m,c}|}{n^2} = \frac{n}{n^2} = \frac{1}{n}$$

$$\therefore \Pr[C=c | M=m] = \Pr[C=c | M=m'] = \frac{1}{n}$$

$$\therefore \Pr[M=m | C=c] = \Pr[M=m'] \text{ for all } m, c$$

Dec: $\text{Dec}_{(k_1, k_2)}(c) = m = (c - k_2) / k_1 \pmod n$

input ciphertext c and key (k_1, k_2)

compute $x = (c - k_2) \pmod n$

if k_1 has an inverse, compute $m = x \cdot k_1^{-1} \pmod n$

else, decryption fails or multiple possible messages

4. 1. E.X. $\text{Enc} : K \times M \rightarrow C$

2. pick any two distinct messages $a, b \in M$ so that $a \neq b$, fix any key $k \in K$

$$u := f_k(a) = \text{Enc}_k(a) \quad v := f_k(b) = \text{Enc}_k(b)$$

by injectivity, $u \neq v$

3. Consider $m_0 = m_1 = a \quad m'_0 = a \quad m'_1 = b \quad c_0 = u, c_1 = v$

$$\therefore \Pr[\text{Enc}(k, a) = u \wedge \text{Enc}(k, b) = v] = 0, \text{ because injectivity}$$

$$\therefore \Pr[\text{Enc}(k, a) = u \wedge \text{Enc}(k, b) = v] > 0$$

\therefore no deterministic encryption scheme with perfect correctness can satisfy the two-time perfect security definition

Need to prove $H(M_0, M_1 | C_0, C_1) = H(M_0, M_1)$