1 Modular Encryption

1.1 Decryption

We have $Dec(k, c) : m = (c - k) \textsf{ mod } n$
To prove correctness, we need to show that $\forall k, m \in \mathbb{Z}_n$, $Dec[k, Enc(k, m)] = m$ holds.

$$\begin{aligned}
Dec[k, Enc(k, m)] &= Dec[k, (k + m) \textsf{ mod } n] \tag{1}\\
&= [(k + m) \textsf{ mod } n - k] \textsf{ mod } n \tag{2}\\
&= (k + m) \textsf{ mod } n - k \textsf{ mod } n \tag{3}\\
&= m \textsf{ mod } n \tag{4}\\
&= m \tag{5}
\end{aligned}$$

1.2 One-time uniform ciphertext security 1

We need to show that $\forall k, m \in \mathbb{Z}_n$, the following distributions $\mathcal{D}_1$ and $\mathcal{D}_2$ are identical:
$\mathcal{D}_1 := \{c := \text{Enc}(k, m); k \leftarrow Z_n\}$ $\mathcal{D}_2 := \{c \overset{\$}{\leftarrow} C\}$
Further, we need to show that $\forall k, m \in \mathbb{Z}_n$ and for arbitrary c, $\Pr[C = c \mid \mathcal{D}_1] = \Pr[C = c \mid \mathcal{D}_2]$

$$\begin{aligned}
\Pr[C = c \mid \mathcal{D}_1] &= \Pr[M = m] = \frac{1}{n} \tag{6}\\
\Pr[C = c \mid \mathcal{D}_2] &= \frac{1}{n} \tag{7}
\end{aligned}$$

Therefore, it satisfies one-time uniform ciphertext security.

1.3 One-time uniform ciphertext security 2

We have the following distributions $\mathcal{D}_1$ and $\mathcal{D}_2$:
$\mathcal{D}_1 := \{c := \text{Enc}(k, m); k \leftarrow \mathbb{Z}_n\}$ $\mathcal{D}_2 := \{c \overset{\$}{\leftarrow} C\}$
We need to construct a calling program by:

$$\begin{aligned}
&\underline{\mathcal{A}}: \tag{8}\\
&\quad c := 0 : \tag{9}\\
&\quad \text{return } c \overset{\$}{\leftarrow} 0 \tag{10}\\
& \tag{11}
\end{aligned}$$

Suppose the plaintext m is 0, then $(c \cdot k) \textsf{ mod } n \equiv 0$ and then we show:

$$\begin{aligned}
\Pr[\mathcal{A} \mid \mathcal{D}_1] &= \Pr[c = 0 \mid \mathcal{D}_1] = 1 \tag{12}\\
\Pr[\mathcal{A} \mid \mathcal{D}_2] &= \Pr[c = 0 \mid \mathcal{D}_2] = \frac{1}{n} \tag{13}
\end{aligned}$$

Clearly the two distributions are not identical and thus the modified scheme does not satisfy one-time uniform ciphertext security.

2 Modified scheme

2.1 One-time uniform ciphertext security

We now have two following distribution: $\mathcal{D}_1 := \{c := \text{Enc}(k, m); k \leftarrow \text{KeyGen}(1^n)\}$ and $\mathcal{D}_2 := \{c \overset{\$}{\leftarrow} C\}$

We need to construct a calling program by:

$$\begin{aligned}
&\underline{\mathcal{A}}: && (14)\\
&\quad c := CTXT(0^n): && (15)\\
&\quad \text{return } c \overset{\$}{\leftarrow} 0^n && (16)\\
& && (17)
\end{aligned}$$

For example, we have $m = 0^n$ and then we show

$$\Pr[\mathcal{A} \mid \mathcal{D}_1] = \Pr[c = 0^n \mid \mathcal{D}_1] = 0 \tag{18}$$

$$\Pr[\mathcal{A} \mid \mathcal{D}_2] = \Pr[c = 0^n \mid \mathcal{D}_2] = \frac{1}{2^n} \tag{19}$$

Clearly the two distributions are not identical and thus the modified scheme does not satisfy one-time uniform ciphertext security.

2.2 One-time perfect security

To prove the insecurity, we need to show $\exists m_0, m_1$ such that the following distributions are not identical: $\mathcal{D}_1 := \{c := \text{Enc}(k, m_0); k \leftarrow \text{KeyGen}(1^n)\}$ and $\mathcal{D}_2 := \{c := \text{Enc}(k, m_1); k \leftarrow \text{KeyGen}(1^n)\}$
Then we have a calling program as:

$$\begin{aligned}
&\underline{\mathcal{A}}: && (20)\\
&\quad c := EAVESDROP(0^n, 1^n): && (21)\\
&\quad \text{return } c \overset{\$}{\leftarrow} 0^n && (22)\\
& && (23)
\end{aligned}$$

For example, we have $m_0 = 0^n$ and $m_1 = 1^n$ and we show

$$\Pr[\mathcal{A} \mid \mathcal{D}_1] = \Pr[c = 0^n \mid \mathcal{D}_1] = 0 \tag{24}$$

$$\Pr[\mathcal{A} \mid \mathcal{D}_2] = \Pr[c = 0^n \mid \mathcal{D}_2] = \frac{1}{2^n - 1} \tag{25}$$

Clearly the two distributions are not identical in this case and thus the modified scheme does not satisfy one-time perfect security.

3 Reordering

Intuitively, the probability by two messages can be identical if and only if they contain the same number of 0s and 1s.
To prove the insecurity, we need to show $\exists m_0, m_1$ such that the following distributions are not identical: $\mathcal{D}_1 := \{c := \text{Enc}(k, m_0); k \leftarrow \mathcal{K}\}$ and $\mathcal{D}_2 := \{c := \text{Enc}(k, m_1); k \leftarrow \mathcal{K}\}$
For $m_0 = 0^n$, $m_1 = 1^n$

$$\Pr[c = 0^n \mid \mathcal{D}_1] = 1 \tag{26}$$

$$\Pr[c = 0^n \mid \mathcal{D}_2] = 0 \tag{27}$$

Clearly the two distributions are not identical in this case and thus the modified scheme does not satisfy one-time perfect security.

4 Two-time Perfect Security

WLOG, suppose the messages and keys are 2-bit. For example, we have $m_{11} = m_{12} = 00$ and $m_{21} = 01$ and $m_{22} = 10$. Now we have

$$\Pr[c_1 = 00, c_2 = 00 \mid \mathcal{D}_1] = \frac{1}{4} \tag{28}$$

$$\Pr[c_1 = 00, c_2 = 00 \mid \mathcal{D}_2] = 0 \tag{29}$$

Clearly the two distributions are not identical in this case and thus the modified scheme does not satisfy two-time perfect security.

5 Combination

Intuitively, we need to remove the impact by the insecure encryption by "transforming" it into a KeyGen algorithm.
Assumption: KeyGen_1 and KeyGen_2 are two independent algorithms. As in the problem, we have

$$k_1 \leftarrow \mathsf{KeyGen}_1 \tag{30}$$

$$k_2 \leftarrow \mathsf{KeyGen}_2 \tag{31}$$

WLOG, we can build a new encryption and a new decryption as

$$Enc^*(k_1, k_2, m) : c = Enc_1(k_1, k_2) \oplus Enc_2(k_2, m)$$

$$Dec^*(k_1, k_2, c) : m = Dec_2(k2, c \oplus Enc_1(k_1, k_2))$$

An encryption scheme (Gen,Enc,Dec) with message space M is perfectly secret [1] if for every probability distribution over M, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $Pr[C = c] > 0$:

$$Pr[M = m|C = c] = Pr[M = m]$$

Before we proceed further proof, we need to define the space size of KeyGen_1 and KeyGen_2 by l_1 and l_2.
Firstly, we show $Pr[C = c|M = m]$ for arbitrary $c \in \mathcal{C}$ and $m \in \mathcal{M}$

$$\begin{aligned} Pr[C = c|M = m] &= Pr[Enc^*_{\mathcal{K}}(m) = c] && (32)\\ &= Pr[Enc_1(k_1, k_2) \oplus Enc_2(k_2, m) = c] && (33)\\ &= Pr[Enc_1(k_1, k_2) = c \oplus Enc_2(k_2, m)] && (34)\\ &= \frac{1}{l_1 \cdot l_2} && (35) \end{aligned}$$

Now we calculate $Pr[C = c]$ by

$$\begin{aligned} \sum_{m \in \mathcal{M}} \Pr[C = c \mid M = m] \cdot \Pr[M = m] &= \frac{1}{l_1 \cdot l_2} \sum_{m \in \mathcal{M}} \Pr[M = m] && (36)\\ &= \frac{1}{l_1 \cdot l_2} \cdot 1 = \frac{1}{l_1 \cdot l_2} && (37) \end{aligned}$$

Now we show $Pr[M = m|C = c]$ by Bayer's Theorem

$$\begin{aligned} Pr[M = m|C = c] &= \frac{Pr[C = c|M = m] \cdot \Pr[M = m]}{Pr[C = c]} && (38)\\ &= \frac{\frac{1}{l_1 \cdot l_2} \Pr[M = m]}{\frac{1}{l_1 \cdot l_2}} && (39)\\ &= \Pr[M = m] && (40) \end{aligned}$$

Therefore, we can conclude that the encryption scheme satisfies one-time perfect security.

6 Extra Credits

Let $\mathcal{K}$, $\mathcal{M}$ and $\mathcal{C}$ be key space, message space and ciphertext space.
Assumption: $|\mathcal{K}| < |\mathcal{M}|$ (there are fewer possible *keys* than there are possible *messages*)
Given a ciphertext c, we should be able to find a message m and key k such that $Enc(k,m) = c$ and $Pr_{k \in \mathcal{K}}[Enc(k,m) = c] > 0$. Since we have fewer keys than messages and each key k can only map one message m to exactly one ciphertext c, there must exist some $m' \in \mathcal{M}$ where there is no possible k' after thoroughly testing on every possible value, to generate ciphertext c, which mathematically is equivalent to $Pr_{k' \in \mathcal{K}}[Enc(k', m') = c] = 0$, which further shows that the difference between m and m'.
To prove the insecurity, we need to show $\exists m_0, m_1$ such that the following distributions are not identical:
$\mathcal{D}_1 := \{c := \text{Enc}(k, m_0); k \leftarrow \mathcal{K}\}$ and $\mathcal{D}_2 := \{c := \text{Enc}(k, m_1); k \leftarrow \mathcal{K}\}$
For example, we have $m_0 = m$ and $m_1 = m'$ where we have already proved the difference previously

$$\Pr[c = c \mid \mathcal{D}_1] > 0 \tag{41}$$
$$\Pr[c = c \mid \mathcal{D}_2] = 0 \tag{42}$$

Clearly the two distributions are not identical in this case and thus the modified scheme does not satisfy one-time perfect security.

References

[1] Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949.