CS152-Homework5

Hongchen Cao 2019533114

2020.10.14

1

Suppose $\textbf{same}(X, X') = j$

For both CBC and CFB mode:

In the first turn, since $y_1 = y'_1$ and using same key and IV, we have $x_1 = x'_1$.

In subsequent turns, for $i^{th}(i \leq j)$ turn, since $x_{i-1} = x'_{i-1}$, $y_i = y'_i$ and using same key, we have $x_i = x'_i$. Until $i = j + 1$, since $y_{j+1} \neq y'_{j+1}$, we have $x_{j+1} \neq x'_{j+1}$.

Thus, adversary get $\textbf{same}(X, X') = j$.

2

For ECB and OFB mode:

Suppose y_j is incorrect, corresponding x_j must be incorrect after decryption.

However, when decrypting other y_i, corresponding x_i just related to y_i and key k_i but have nothing to do with y_j, x_j.

Thus, equal to one.

For CBC and CFB mode:

Suppose y_j is incorrect, corresponding x_j must be incorrect after decryption. Now consider x_{j+1}, it depends on y_{j+1}, k_{j+1} and y_j. However y_j is incorrect, so y_{j+1} is incorrect.

When decrypting other $y_i(i \neq j, j + 1)$, corresponding x_i related to y_i, k_i and y_{i-1} but have nothing to do with y_j, x_j, x_{j+1}.

Thus, equal to two.

3

Res:

[0 0 0 0 1 1 1]

[0 0 1 1 1 1 0]

[0 1 0 1 1 0 1]

[0 1 1 0 1 0 0]

[1 0 0 1 0 1 1]

[1 0 1 0 0 1 0]

[1 1 0 0 0 0 1]

[1 1 1 1 0 0 0]

Code:

```
import numpy as np


def getPreimages(hashMatrix, image):
    res = list()
    for i in range(pow(2, 7)):
        preimage = np.array([int(j) for j in list('{:07b}'.format(i))]) % 2
        tempImage = np.matmul(preimage, hashMatrix) % 2

        if (tempImage == image).all():
            res.append(preimage)
    return res


if __name__ == '__main__':
    A = np.array([[1, 0, 0, 0], [1, 1, 0, 0], [1, 1, 1, 0], [1, 1, 1, 1], [0, 1, 1, 1], [
                                                 0, 0, 1, 1], [0, 0, 0, 1]])
    image = np.array([0, 1, 0, 1])
    for arr in getPreimages(A, image):
        print(arr)
```

4

Suppose,

$$\nexists \hat{x} \neq x : h(x) = h(\hat{x}) \Rightarrow \forall \hat{x} \in \{0,1\}^m : \hat{x} \neq x \Rightarrow h(x) \neq h(\hat{x}) \Rightarrow f(x' \oplus x'') \neq f(\hat{x}' \oplus \hat{x}'') \tag{1}$$

Since f is bijection, we have

$$f(x' \oplus x'') \neq f(\hat{x}' \oplus \hat{x}'') \Rightarrow x' \oplus x'' \neq \hat{x}' \oplus \hat{x}'', \forall x, \hat{x} \in \{0,1\}^m \tag{2}$$

However, we can easily find a counterexample like $x = 10100010$ and $\hat{x} = 01101100$. So we have:

$$x' \oplus x'' = 1010 \oplus 0010 = 1000 \tag{3}$$

$$\hat{x}' \oplus \hat{x}'' = 0100 \oplus 1100 = 1000 \tag{4}$$

Thus, contradiction happens so we proved h is not second preimage resistant.