CS152-Homework7

Hongchen Cao 2019533114

2020.11.6

1

Under CFB mode:

$$
\begin{aligned}
IV &= x_1 && (1)\\
y_1 &= e_K(x_1) \oplus x_2 && (2)\\
y_2 &= e_K(y_1) \oplus x_3 && (3)\\
y_3 &= e_K(y_2) \oplus x_4 && (4)\\
&\vdots && (5)\\
y_{n-1} &= e_K(y_{n-2}) \oplus x_n && (6)\\
\mathbf{MAC} &= e_K(y_{n-1}) && (7)
\end{aligned}
$$

Under CBC mode with $IV = 00\ldots0$:

$$
\begin{aligned}
IV &= 00\ldots0 && (8)\\
y'_1 &= e_K(x'_1) && (9)\\
y'_2 &= e_K(y'_1 \oplus x_2) && (10)\\
y'_3 &= e_K(y'_2 \oplus x_3) && (11)\\
&\vdots && (12)\\
y'_n &= e_K(y'_{n-1} \oplus x_n) && (13)\\
\mathbf{MAC}' &= y'_n && (14)
\end{aligned}
$$

By induction we have $y_i = y'_i \oplus x_{i+1}$, $1 \le i \le n-1$
Finally we have $\mathbf{MAC} = e_K(y_{n-1}) = e_K(y'_{n-1} \oplus x_n) = y'_n = \mathbf{MAC}'$

2

$P_{d_0} = \frac{1}{2}$; the pair $(4,1)$
Let a_{ij} be the probability of forging a MAC, we get a table

Then, $P_{d_1} = \frac{1}{2}$

i	**j**	a_{ij}	optimal forgery
1	1	1/2	(2,1)
1	2	1/2	(2,1)
1	3	1/2	(2,2)
2	1	1/2	(1,1)
2	2	1/2	(1,1)
2	3	1/2	(1,2)
3	1	1/2	(1,2)
3	2	1/2	(1,1)
3	3	1	(4,1)
4	1	2/3	(3,3)
4	2	1	(1,2)
4	3	1/2	(1,1)

3

Suppose that $x, x', y, y' \in \mathbb{Z}_p$, where $x \neq x'$.
Suppose (a, b) is a key $\in \mathbb{Z}_p \times \mathbb{Z}_p$

$$(x+a)^2 + b \equiv y (mod\ p) \tag{15}$$

$$(x'+a)^2 + b \equiv y' (mod\ p) \tag{16}$$

Then we have

$$(x+a)^2 - (x'+a)^2 \equiv y - y' (mod\ p) \tag{17}$$

$$x^2 - (x')^2 + 2a(x - x') \equiv y - y' (mod\ p) \tag{18}$$

$$x + x' + 2a \equiv (y - y')(x - x')^{-1} (mod\ p) \tag{19}$$

$$a = 2^{-1}((y - y')(x - x')^{-1} - (x + x'))\ mod\ p. \tag{20}$$

Now a is unique so that b also can be calculated uniquely.
Thus, key (a, b) is unique.

4

Suppose $x \not\equiv 0\ (mod\ p)$. Then for some positive int k, we have

$$x^{ab} = x^{1+k(p-1)(q-1)} \equiv x \times x^{k(p-1)(q-1)} \equiv x\ (mod\ p)$$

If $x \equiv 0\ (mod\ p)$, then $x^{ab} \equiv x \equiv 0\ (mod\ p)$.
Similarly, $x^{ab} \equiv x\ (mod\ q)$ for any $x \in \mathbb{Z}_q$.
By the Hint we know have $x^{ab} \equiv x\ (mod\ n)$ for any $x \in \mathbb{Z}_n$