Ex 24: Block Cipher Hash Functions

Block cipher with block length k, $m = (\overbrace{m_0, \ldots, m_{n-1}}^{k})$ zero-padded

and the following hash function h:

$c \leftarrow E_{m_0}(m_0)$

for $i = 1, \ldots, n-1$

$d \leftarrow E_{m_0}(m_i)$

$c \leftarrow c \oplus d$

end for

$h(m) \leftarrow c$

Take $m = m_0$ and $\hat{m} = (m_0, m_1, m_1)$ m_0, m_1 arbitrary

$\Rightarrow h(\hat{m}) = E_{m_0}(m_0) \oplus \underbrace{E_{m_0}(m_1) \oplus E_{m_0}(m_1)}_{=0} = E_{m_0}(m_0) = h(m)$ // elementary boolean algebra

$\Rightarrow$ h is neither collision-free, nor second preimage resistant

$\Rightarrow$ requirements are <u>not</u> fulfilled

The modified hash function $\hat{h}$ replaces Xor ($\oplus$) by And ($\odot$)

$\Rightarrow$ Take $m = (m_1, m_1)$ m_1 arbitrary

$\Rightarrow \hat{h}(m) = E_{m_1}(m_1) \odot E_{m_1}(m_1) = E_{m_1}(m_1) = \hat{h}(m_1)$

$\Rightarrow$ $\hat{h}$ is neither collision-free, nor second preimage resistant.

Ex 25: Message Authentification (MAC)

Example 10.5 provides:

Given $\hat{\zeta}_0 = 0$ // initial value (1)

K // key

$M_1, \dots, M_n$ // Message with n blocks

CBC // Cipher blockchaining mode

$$\hat{\zeta}_i = E_K(\hat{\zeta}_{i-1} \oplus M_i) \quad , i = 1, \dots, n \quad (2)$$

$$\Rightarrow \hat{MAC}_K^{(n)} = \hat{\zeta}_n \quad (3)$$

CFB // Cipher feedback mode

$$\zeta_0 = M_1 \quad (4)$$

$$\hat{M}_i = M_{i+1} \quad , i = 2, \dots, n \quad (5)$$

$$Z_i = E_K(\zeta_{i-1}) \quad , i = 2, \dots, n \quad (6)$$

$$\zeta_i = \hat{M}_i \oplus Z_i \quad , i = 2, \dots, n \quad (7)$$

$$\Rightarrow MAC_K^{(n)} = E_K(\zeta_{n-1}) \quad (8)$$

Claim: $$MAC_K^{(n)} = \hat{MAC}_K^{(n)} \quad (9)$$

Proof: Induction over n

$n = 1$:

$$\hat{MAC}_K^{(1)} \overset{(3)}{=} \hat{\zeta}_1 \overset{(2)}{=} E_K(\hat{\zeta}_0 \oplus M_1) \overset{(1)}{=} E_K(M_1) \overset{(4)}{=} E_K(\zeta_0) \overset{(8)}{=} MAC_K^{(1)}$$

$n \to n+1$:

$$MAC_K^{(n+1)} \overset{(8)}{=} E_K(\zeta_n) \overset{(7)}{=} E_K(\hat{M}_n \oplus Z_n) \overset{(5),(6)}{=} E_K(M_{n+1} \oplus E_K(\zeta_{n-1}))$$

$$\overset{(8)}{=} E_K(M_{n+1} \oplus MAC_K^{(n)}) \overset{(9)}{=} E_K(M_{n+1} \oplus \hat{MAC}_K^{(n)}) \overset{(3)}{=} E_K(M_{n+1} \oplus \hat{\zeta}_n) \overset{(2)}{=} \hat{\zeta}_{n+1}$$

$$\overset{(3)}{=} \hat{MAC}_K^{(n+1)} \qquad \square$$

Ex 26: Hash-functions and ElGamal Signatures

a) given: $m = (3, 33, 13, 25)$, $\ell = 4$, $n = 221 = 13 \cdot 17$

calculate:

$h(m) = h_4$

$h_0 = 0$

$h_1 \equiv 2^{(h_0 + m_1)} \pmod n \equiv 2^3 \equiv 8 \pmod{221}$

$h_2 \equiv 2^{8+33} \equiv 2^{41} \equiv 2^1 \cdot 2^{10} \cdot 2^{10} \cdot 2^{10} \cdot 2^{10}$

$\equiv \underbrace{2 \cdot 140}_{59} \cdot \underbrace{140 \cdot 140 \cdot 140}_{64}$ // $2^{10} \equiv 1024 \equiv 140 \pmod{221}$

$\equiv 19 \pmod{221}$

$h_3 \equiv 2^{19+13} \equiv 2^{32} \equiv 2^2 \cdot 2^{10} \cdot 2^{10} \cdot 2^{10}$

$\equiv 4 \cdot 64 \equiv 35 \pmod{221}$

$h_4 \equiv 2^{35+25} \equiv 2^{60} \equiv 2^{30} \cdot 2^{30} \equiv 64 \cdot 64 \equiv 118 \pmod{221}$

$\Rightarrow h(m) = 118$

b) Sign hash with ElGamal Signature Scheme

Parameters:

$p = 4793$ // prime number

$x_A = 9177$ // private key $x_A \in \mathbb{Z}_p^*$

$a = 4792$

1.) check if p is prime: 4793 ✓ // by MRPT or divide all primes $< \sqrt{p}$

2.) check if a is a PE mod p:

apply Prop. 7.5 $\Rightarrow p - 1 = \prod_{i=1}^{k} p_i^{t_i}$

// a is PE $\Leftrightarrow a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod p \quad \forall i \in \{1, \dots, k\}$ //

check $a \equiv 4792 \equiv -1 \pmod{4793}$

$\Rightarrow a^2 \equiv 1 \pmod{4793}$ ✓

check $a = 1400$ with $p - 1 = 4792 = 2^3 \cdot 599$

1. $p_1 = 2 \Rightarrow 1400^{\frac{4792}{2}} \equiv 4792 \not\equiv 1 \pmod{4793}$ ✓

2. $p_2 = 599 \Rightarrow 1400^{\frac{4792}{599}} \equiv 2691 \not\equiv 1 \pmod{4793}$ ✓

$\Rightarrow a = 1400$ is a PE mod p ✓

$\Rightarrow$ choose $a = 1400$

3.) check: $x_A \in \mathbb{Z}_p^*$: $x_A = 9177 \in \mathbb{Z}_{4793}^*$ ↙ // $x_A \notin \mathbb{Z}_{4793}$

$x_A = 257 \in \mathbb{Z}_{4793}^*$ ✓ // $x_A \in \mathbb{Z}_{4793}$ and $\gcd(257, 4793) = 1$ ✓

$\Rightarrow x_A = 257$ ✓

4.) check $\gcd(k, p-1) = 1$ ✓ // relatively prime

5.) Sign hash of message

$p = 4793,\ a = 1400,\ x_A = 257,\ h(m) = 118,\ k = 2811$ (k: session key)

- $r \equiv a^k \pmod{p} \equiv 1400^{2811} \pmod{4793} \equiv 2666$ // Square & Multiply
- $k^{-1} \pmod{(p-1)} \equiv -1045 \equiv 3747 \pmod{4792}$ // EEA
- $s \equiv k^{-1}(h(m) - x_A r) \pmod{(p-1)} \equiv -1045(118 - 257 \cdot 2666) \bmod p-1$

$\equiv 3684 \pmod{4792}$

$\Rightarrow \langle r, s \rangle = \langle 2666, 3684 \rangle$