Solution Sheet 9

Cryptography and Security 2022

Solution 1 MAC From Hash Functions

1. Use $1\|0\ldots0\|\delta$ where the number of 0's is the smallest positive λ such that $1+\lambda+64 \equiv 0 \mod \ell$ and δ denotes the bit-length of the message encoded on 64 bits.

2. (a) Resistance to preimage attack
   (b) Resistance to 2nd preimage attack
   (c) Resistance to collisions

3. A MAC forgery is an attack in which an adversary *not* knowing the secret key K tries to forge a pair (m, c) such that $\mathsf{Verify}_K(m, c) = 1$.

   The security models for such an attack are:

   (a) known message attack
   (b) chosen message attack

4. **The Prefix Method**. Let us define the message $m' = m\|\mathsf{pad}(m)\|m^\star$ for any message $m^\star$.

   Then the adversary can compute the MAC of m' by hashing $m^\star$ and using $\mathsf{IV} = \mathsf{MAC}_K(m)$.

5. **The Suffix Method**. Notice first that

$$H_0(m_1\|\mathsf{pad}(m_1)) = H_0(m_2\|\mathsf{pad}(m_2)) \implies \mathsf{MAC}_K(m_1) = \mathsf{MAC}_K(m_2)$$

   The attack then consists of submitting m_1 to the MAC Oracle and get $\mathsf{MAC}_K(m_1)$ which is also the MAC of m_2.

Solution 2 Collisions with a Subset

1. The probability that we have no collision is

$$1 \cdot \left(1 - \frac{1}{N}\right) \cdot \left(1 - \frac{2}{N}\right) \cdots \left(1 - \frac{x-1}{N}\right) = \frac{N!}{N^x(N-x)!}$$

   So, the probability to have a female-female collision is

$$p_{xx} = 1 - \frac{N!}{N^x(N-x)!}$$

2. The probability of no female-male collision under the condition that there are exactly x female birthdays is $\left(1 - \frac{x}{N}\right)^y$. So, the probability to have a male-female collision is

$$p_{xy|\neg xx} = 1 - \left(1 - \frac{x}{N}\right)^y$$

3. We have

$$p_{xy|\neg xx} = 1 - e^{y \log\left(1 - \frac{x}{N}\right)}$$

   Since $\log(1-\varepsilon) \approx -\varepsilon$, we obtain the result.

4. It is

$$p_{x\star} = p_{xx} + (1 - p_{xx})p_{xy|\neg xx} = 1 - \frac{N!}{N^x(N-x)!} + \frac{N!}{N^x(N-x)!}\left(1 - \left(1 - \frac{x}{N}\right)^y\right)$$

5. We have

$$p_{x\star} = p_{xx} + (1 - p_{xx})p_{xy|\neg xx} \approx 1 - e^{-\frac{x^2}{2N}} + e^{-\frac{x^2}{2N}}\left(1 - e^{-\frac{xy}{N}}\right) = 1 - e^{-\frac{x(x+2y)}{2N}}$$

6. We take $x = n_u$ and $y = n_t$. The attacker succeeds if either there is a collision between the list x and the list y, or there is a collision inside the list x. If the range of the hash function is N, this probability is thus $p_{x\star}$.

Solution 3 CBCMAC and Variants

1. Given some (known or chosen) sample pairs message-code (m_i, c_i), the goal of a MAC forgery attack is to output a valid pair message-code (m, c).

2. It is simply $\mathcal{O}(2^n)$.

3. Since there is a xor between one message block let x_i and the result of $\mathsf{CBCMAC}(K, x_1, \ldots, x_{i-1})$ they should have the same bit length:

$$n = b \ .$$

4. As seen in the course:

   - choose m_1 and obtain $c_1 \leftarrow \mathsf{CBCMAC}(K, m_1)$
   - choose m_2 and obtain $c_2 \leftarrow \mathsf{CBCMAC}(K, m_2)$
   - choose B_1, let $m'_1 = m_1 \| B_1$ and obtain $c'_1 \leftarrow \mathsf{CBCMAC}(K, m'_1)$
     Note that $c'_1 = \mathsf{CBCMAC}(K, B_1 \oplus \mathsf{CBCMAC}(K, m_1)) = \mathsf{CBCMAC}(K, B_1 \oplus c_1)$
   - let $m'_2 = m_2 \| B_2$ for some B_2
     Note that c'_2 should be $\mathsf{CBCMAC}(K, B_2 \oplus \mathsf{CBCMAC}(K, m_2)) = \mathsf{CBCMAC}(K, B_2 \oplus c_2)$
     So, if $B_2 \oplus c_2 = B_1 \oplus c_1$ then $c'_2 = c'_1$
     Fix $B_2 = B_1 \oplus c_1 \oplus c_2$
   - output $(m2 \| B_2, c'_1)$

   Note that it is possible to design a simpler attack:

   - Choose m_1 at random and obtain $c_1 \leftarrow \mathsf{CBCMAC}(K, m_1)$
   - The message $m_1 \| m_1 \oplus c_1$ has the same MAC.