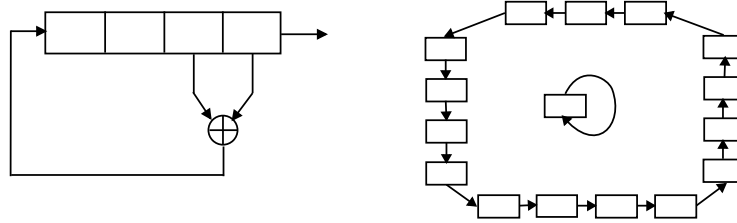


Solutions to Assignment 6 (Topic 8)

Question 1

(a) Since the PRSG is an LFSR with the characteristic polynomial $x^4 + x + 1$ with an initial state $(a_0, a_1, a_2, a_3) = 0001$, we can obtain the following state transition diagram:



Assume that Alice and Bob generate the challenge numbers $R_A = 1010$ and $R_B = 1111$, respectively, from the above PRSG. Then the authentication tags can be calculated as follows:

$$\begin{aligned} \text{Tag}_B &= \text{MAC}(K, ID_B, ID_A, R_B, R_A) = f(1100 \oplus 1101 \oplus 0101 \oplus 1111 \oplus 1010) \\ &= f(0001) = 0001, \\ \text{Tag}_A &= \text{MAC}(K, ID_A, R_B) = f(1100 \oplus 0101 \oplus 1111) = f(0110) = 0111. \end{aligned}$$

(b) Firstly, an attacker E can use the vulnerability of the given MAC function to derive the pre-shared key between A and B and therefore impersonates A as follows:

- (i) The attacker E first chooses a random challenge number R_A (for example $R_A = 0000$) and sends ID_A and R_A to B .
- (ii) B chooses a random challenge number R_B (for example $R_B = 0001$) and calculates the authentication tag Tag_B as follows:

$$\begin{aligned} \text{Tag}_B &= \text{MAC}(K, ID_B, ID_A, R_B, R_A) = f(1100 \oplus 1101 \oplus 0101 \oplus 0001 \oplus 0000) \\ &= f(0101) = 1011. \end{aligned}$$

Then B sends ID_B, ID_A, R_B, R_A and the authentication tag Tag_B to A .

- (iii) Since the MAC function is known to everyone, the attacker E can look up the table and find the preimage of the Tag_B which is 0101. Therefore, the attacker E can derive the pre-shared key K between A and B as follows:

$$\begin{aligned} K &= f^{-1}(\text{Tag}_B) \oplus ID_B \oplus ID_A \oplus R_B \oplus R_A \\ &= 0101 \oplus 1101 \oplus 0101 \oplus 0001 \oplus 0000 = 1100. \end{aligned}$$

- (iv) With the pre-shared key K , the attacker E can impersonate A to generate the correct authentication tag Tag_A as follows:

$$\text{Tag}_A = \text{MAC}(K, ID_A, R_B) = f(1100 \oplus 0101 \oplus 0001) = f(1000) = 1111.$$

Then E sends ID_A, R_B and the authentication tag Tag_A to B .

- (v) B will accept the attacker E as A .

Secondly, since the period of the given PRSG is very small, A can only generate 16 different authentication tags for a given pre-shared key K . Therefore, the probability that a tag will be reused by A is $\frac{1}{16}$, which is not negligible. So an attacker E can impersonate A by launching the replay attack in this case.

(c) To thwart the above attacks, we should choose a secure hash function (i.e., SHA-1) to generate authentication tags and a secure PRSG (i.e., RC4) to generate challenge numbers.