Introduction to Cryptography: Assignment 1

Group number 57

Elwin Tamminga
s1013846

Lucas van der Laan
s1047485

1

(a) Because the server can not authenticate the client, a man-in-the-middle attack can be achieved. An adversary also has access to the shared key because the client is not authenticated towards the server. Because the adversary has access to the shared key, they can decrypt the messages which leads to a loss of confidentiality.

(b) Yes, because the public keys used for the signature schemes are authenticated, the server can verify using the public key of the client that the message is signed by the client's private key. If the signature is valid, we can verify that the message has not been modified.

(c) Yes, assuming the client's private key is not leaked, the server can assume that the signed message came from the client using the public key, who used their private key to create the signature.

2

(a)

$$M = \begin{pmatrix} . & . & . & 1 \\ 1 & . & . & . \\ . & 1 & . & . \\ . & . & 1 & 1 \end{pmatrix}$$

(b) *Given states are from iteration 0 (s^0)*

$$s^1 = \begin{pmatrix} s_3 \\ s_0 \\ s_1 \\ s_2 + s_3 \end{pmatrix}$$

$$s^2 = \begin{pmatrix} s_2 + s_3 \\ s_3 \\ s_0 \\ s_1 + (s_2 + s_3) \end{pmatrix}$$

$z_2 = s_1 + s_2 + s_3$

(c) *Given states are from iteration 0 (s^0)*

$$s^3 = \begin{pmatrix} s_1 + (s_2 + s_3) \\ s_2 + s_3 \\ s_3 \\ s_0 + (s_1 + (s_2 + s_3)) \end{pmatrix}$$

$z_3 = s_0 + s_1 + s_2 + s_3$

(d)

$$\begin{aligned} s^t &= M^t * s^0 \\ z_t &= s_3^t \end{aligned}$$

$$M^2 = M * M = \begin{pmatrix} . & . & 1 & 1 \\ . & . & . & 1 \\ 1 & . & . & . \\ . & 1 & 1 & 1 \end{pmatrix}$$

$$M^3 = M * M^2 = \begin{pmatrix} . & 1 & 1 & 1 \\ . & . & 1 & 1 \\ . & . & . & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

$$M^6 = M^3 * M^3 = \begin{pmatrix} 1 & 1 & . & 1 \\ 1 & 1 & 1 & . \\ 1 & 1 & 1 & 1 \\ 1 & . & 1 & . \end{pmatrix}$$

$$M^8 = M^6 * M^2 = \begin{pmatrix} . & 1 & . & 1 \\ 1 & . & 1 & . \\ 1 & 1 & . & 1 \\ 1 & . & 1 & 1 \end{pmatrix}$$

$$M^{14} = M^6 * M^8 = \begin{pmatrix} . & 1 & . & . \\ . & . & 1 & . \\ 1 & . & . & 1 \\ 1 & . & . & . \end{pmatrix}$$

$$\begin{aligned} z_3 &= s_0 + s_1 + s_2 + s_3 \\ z_6 &= s_0 + s_2 \\ z_8 &= s_0 + s_2 + s_3 \\ z_{14} &= s_0 \\ z &= (z_3, z_6, z_8, z_{14})^T \\ &= ((s_0 + s_1 + s_2 + s_3), (s_0 + s_2), (s_0 + s_2 + s_3), (s_0))^T \\ &= \begin{pmatrix} s_0 + s_1 + s_2 + s_3 \\ s_0 + s_2 \\ s_0 + s_2 + s_3 \\ s_0 \end{pmatrix} \\ N &= \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & . & 1 & . \\ 1 & . & 1 & 1 \\ 1 & . & . & . \end{pmatrix} \end{aligned}$$

(e)

$$s^0 = N^{-1} * z$$

$$N * N^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

$$R_2 = R_2 - R_1$$

$$R_3 = R_3 - R_1$$

$$R_4 = R_4 - R_1$$

$$\rightarrow \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 & -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & -1 & -1 & -1 & -1 & 0 & 0 & 1 \end{array}\right)$$

$$R_2 = R_2 * -1$$

$$\rightarrow \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & -1 & -1 & -1 & -1 & 0 & 0 & 1 \end{array}\right)$$

$$R_3 = R_3 + R_2, R_4 = R_4 + R_2$$

$$\rightarrow \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 & -1 & 0 & 1 \end{array}\right)$$

$$R_4 = R_4 * -1$$

$$\rightarrow \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & -1 \end{array}\right)$$

$$R_4 \longleftrightarrow R_3$$

$$\rightarrow \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & -1 & 1 & 0 \end{array}\right)$$

$$R_1 = R_1 - R_2 - R_3$$

$$\rightarrow \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & -1 & 1 & 0 \end{array}\right)$$

$$R_2 = R_2 - R_4$$

$$\rightarrow \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & -1 & 1 & 0 \end{array}\right)$$

$$N^{-1} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{pmatrix}$$

$$N^{-1} * z = s^0$$

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{pmatrix} * \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0*1+0*1+0*0+1*1 & =1 \\ 1*1+0*1+-1*0+0*1 & =1 \\ 0*1+1*1+0*0+-1*1 & =0 \\ 0*1+-1*1+1*0+0*1 & =1 \end{pmatrix}$$