Intro to Crypto Assignment 1

Jan Hendron(s1049777), Nick Weibe(s4163168)

September 2021

Question 1

(a) Confidentiality is maintained, as since the client has a authenticated the server, and the server has the public key of the client, the client can ensure that only the server can decrypt any messages sent to it.

(b) Data integrity is maintained, since a signature is used, and as such any alteration to the original message will mean that the signature is changed, and as such both the server and the client can ensure that the original messages that they both sent will not be altered by an attacker.

(c) Origin authentication is not secured in this scenario, as since the client is never authenticated by the server, the server has no way of knowing if the message that is sent is actually sent by the client that it has established a connection with. However, since the client has authenticated the server, it is harder for an attacker to gain certain information from any messages sent between the 2 parties, as the client can ensure that it is receiving responses from the server

Question 2

(a) $$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

(b) $$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{pmatrix} = \begin{pmatrix} s_2 + s_3 \\ s_3 \\ s_0 \\ s_1 + s_2 + s_3 \end{pmatrix} \implies z_2 = s_1 + s_2 + s_3$$

(c) $$\begin{pmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&1\end{pmatrix}\cdot\begin{pmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&1\end{pmatrix}\cdot\begin{pmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&1\end{pmatrix}=\begin{pmatrix}0&1&1&1\\0&0&1&1\\0&0&0&1\\1&1&1&1\end{pmatrix}$$

$$\begin{pmatrix}0&1&1&1\\0&0&1&1\\0&0&0&1\\1&1&1&1\end{pmatrix}\cdot\begin{pmatrix}s_0\\s_1\\s_2\\s_3\end{pmatrix}=\begin{pmatrix}s_1+s_2+s_3\\s_2+s_3\\s_3\\s_1+s_2+s_3+s_4\end{pmatrix}\Longrightarrow z_3=s_1+s_2+s_3+s_4$$

(d) Approach: find z_3, z_6, z_8, z_{14} using the procedure from (b) and (c). Then find the matrix N such that

$$N\cdot\begin{pmatrix}s_0\\s_1\\s_2\\s_3\end{pmatrix}=\begin{pmatrix}z_3\\z_6\\z_8\\z_{14}\end{pmatrix}$$

We know from (c) that $z_3 = s_1 + s_2 + s_3 + s_4$

The others we have to compute:

$$z_6:\begin{pmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&1\end{pmatrix}^6\cdot\begin{pmatrix}s_0\\s_1\\s_2\\s_3\end{pmatrix}=\begin{pmatrix}s_0+s_1+s_3\\s_0+s_1+s_2\\s_0+s_1+s_2+s_3\\s_0+s_2\end{pmatrix}\Longrightarrow z_6=s_0+s_2$$

$$z_8:\begin{pmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&1\end{pmatrix}^8\cdot\begin{pmatrix}s_0\\s_1\\s_2\\s_3\end{pmatrix}=\begin{pmatrix}s_1+s_3\\s_0+s_2\\s_0+s_1+s_3\\s_0+s_2+s_3\end{pmatrix}\Longrightarrow z_8=s_0+s_2+s_3$$

$$z_{14}:\begin{pmatrix}0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&1\end{pmatrix}^{14}\cdot\begin{pmatrix}s_0\\s_1\\s_2\\s_3\end{pmatrix}=\begin{pmatrix}s_1\\s_2\\s_0+s_3\\s_0\end{pmatrix}\Longrightarrow z_{14}=s_0$$

We want a matrix N such that $N\cdot\begin{pmatrix}s_0\\s_1\\s_2\\s_3\end{pmatrix}=\begin{pmatrix}s_0+s_1+s_2+s_3\\s_0+s_2\\s_0+s_2+s_3\\s_0\end{pmatrix}=\begin{pmatrix}z_3\\z_6\\z_8\\z_{14}\end{pmatrix}$

So N clearly is this matrix: $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$

(e) $z_3 = 1 = s_0 + s_1 + s_2 + s_3$
$z_6 = 1 = s_0 + s_2$
$z_8 = 0 = s_0 + s_2 + s_3$
$z_{14} = 1 = s_0$
From z_{14} we know that $s_0 = 1$. Then from z_6 we know that $1 = 0 + s_2$ so $s_2 = 1$. Then from z_8 we know that $0 = 0 + 1 + s_3$ so $s_3 = 1$. Then from z_3 we know that $1 = 1 + s_1 + 1 + 1$, so $s_1 = 0$

So the initial state is $(1, 0, 1, 1)$.