1 Tutorial 7

1. Let $a = 1234, b = 4321$ and $m = 42$. Demonstrate how you can use the Chinese Remainder Theorem (crt) to compute $a + b \bmod m$ and $b^{769} \bmod m$ using a representation with moduli $m_i = \{2, 3, 7\}$.

2. Suppose Pablo and Renee share a symmetric secret key and generate a fresh session key every hour whenever they need to communicate. Assume that Pablo and Renee use different machines on different networks on the Internet. Under this scheme, Pablo sends to Renee the message to "pay John $1000". How can an intruder exploit this scheme? Explain any improvements.

3. The symmetric key exchange protocol using a trusted server (page 3 of notes) uses a nonce I_p. Suppose we simplify the protocol to remove the use of I_p, we may argue for example that I_p is not used by P or R. This new protocol is less secure than the original one. Explain a possible attack. What assumptions do you need?

4. Consider a session key exchange scheme with RSA using the following following protocol where K_{PR} is the session key generated by P, K^P_{pub} denotes the public key of P and K^P_{priv} denotes the private key of P, and encryption and decryption with those RSA keys is denoted by E_P and D_P respectively:

$$
\begin{aligned}
&P \to R : (P, K^P_{pub}) \\
&R \to P : (R, K^R_{pub}) \\
&P \to R : (P, I_P, E_R(K_{PR})) \\
&R \to P : (R, E_P(I_P))
\end{aligned}
$$

   Show how an adversary who has control of the network can obtain the session key K_{PR}.