1. [14 points]
Are n=323 and e=5 valid numbers for RSA. Explain. If you answer yes, obtain the corresponding d.
2. [5 points]
Recall that a DES encryption operation takes a 64-bit plaintext block and a 56-bit key and produces a 64-bit ciphertext block. Recall also that each DES encryption operation itself consists of a number of iterations, which we shall refer to as basic iterations.

For the DES encryption in CBC mode of a plaintext message of N 64-bit blocks, obtain the following (in terms of N):

a. Total number of DES encryption operations.
b. Size of the output. Explain briefly.
c. Total number of basic iterations. Explain briefly.
3. [6 points]
Is there an integer $K$ in the range 1, ..., 47 such that $K^{48} \mod 105$ is not equal to 1?
If you answer yes, produce such a $K$ and the value of $K^{48} \mod 105$ (as an integer in the range 1, ..., 47).
If you answer no, explain.
4. [10 points]
Consider a public key infrastructure with principals A₁, A₂, ..., A₂₀ and B₁, B₂, ..., B₂₀. There are three certification authorities, namely, X, Y, and Z. Each principal (i.e., Aᵢ and Bᵢ) has X’s public key. X issues certificates for Y and Z. Y issues certificates for A₁, A₂, ..., A₂₀. Z issues certificates for B₁, B₂, ..., B₂₀.

Suppose A₁ wants the public key of B₂. What are the documents (e.g., certificates) that A₁ looks for. For each document, describe its fields and any constraints that must hold.
5. [10 points]
The chart below shows a skeleton of an authentication protocol. Initially, principals A and B share a secret key K and public Diffie-Hellman parameters g and p. Assume an attacker that can eavesdrop, intercept messages, and send messages with another’s sender id. Supply an authentication protocol (i.e., the part indicated by the “● ● ● ●”) such that:
- A initiates the protocol.
- A and B authenticate each other (i.e., the attacker cannot impersonate one to the other).
- A and B establish a session key S (for encrypting data) such that after A and B disconnect and forget S, even if the attacker learns K, the attacker cannot decrypt the data exchanged.
- The authentication involves at most 4 messages (it can be fewer). (Only one cell can be used in each row.)

<table>
<thead>
<tr>
<th>A (has K, g, p)</th>
<th>B (has K, g, p)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<------------------- A and B exchange data ----------------->

<------------------- A and B disconnect ------------------->
In the authentication protocol below, pw is A's password and J is a key derived from pw.

<table>
<thead>
<tr>
<th>A (has pw)</th>
<th>B (has J)</th>
</tr>
</thead>
<tbody>
<tr>
<td>send [A, B, conn] // msg 1</td>
<td>receive [A, B, conn]</td>
</tr>
<tr>
<td></td>
<td>generate random challenge $R_B$</td>
</tr>
<tr>
<td></td>
<td>$S_B \leftarrow$ encrypt($R_B$) with key $J$</td>
</tr>
<tr>
<td></td>
<td>send [B, A, $S_B$] // msg 2</td>
</tr>
</tbody>
</table>

receive [B, A, $S_B$]
compute $J$ from pw
$T_B \leftarrow$ decrypt($S_B$) with key $J$
$U_B \leftarrow$ encrypt($T_B+1$) with key $J$
generate random challenge $R_A$
$S_A \leftarrow$ encrypt($R_A$) with key $J$
send [A, B, $U_B$, $S_A$] // msg 3

receive [A, B, $U_B$, $S_A$]
$V_B \leftarrow$ decrypt($U_B$) with key $J$
if $V_B = R_B+1$ then A is authenticated else abort
$T_A \leftarrow$ decrypt($S_A$) with key $J$
$U_A \leftarrow$ encrypt($T_A+1$) with key $J$
send [B, A, $U_A$] // msg 4

receive [B, A, $U_A$]
$V_A \leftarrow$ decrypt($U_A$) with key $J$
if $V_A = R_A+1$ then B is authenticated else abort

a. Consider an attacker that can only eavesdrop (i.e., can hear messages in transit but cannot intercept messages or send messages with somebody else's sender id). Can this attacker obtain pw by off-line password guessing. If you answer no, explain briefly. If you answer yes, describe the attack.

b. Consider an attacker that can only spoof A (i.e., send messages with sender id A and receive messages with destination id A, but not eavesdrop or intercept messages). Can this attacker obtain pw by off-line password guessing. If you answer no, explain briefly. If you answer yes, describe the attack.

c. Consider an attacker that can only spoof B (i.e., send messages with sender id B and receive messages with destination id B, but not eavesdrop or intercept messages). Can this attacker obtain pw by off-line password guessing. If you answer no, explain briefly. If you answer yes, describe the attack.