CS2362: Computer Security and Privacy (Spring 2024), Mahavir Jhawar, Ashoka University						
Date	_			Maximum Marks	Weightage	
April 13, 2024	10 PM	CS2362_A4	40	40	10%	

## # Submission Instructions

- -Submit a compressed folder containing the programs  $\,$
- Name your folder as follows: yourname\_CS2362\_A4.zip

## **Submission Link - TBA**

1. Write client and server programs to implement the following functionality:

	Client		Server
1		Client hello message	
1		hello	1001:
			Generate a 128-bit prime p
$_2$			Consider the group $G = \mathbb{Z}_p^*$ Pick a $g \in \mathbb{Z}_p^*$ such that $\langle g \rangle = \mathbb{Z}_p^*$
Δ			Pick a $\alpha \leftarrow \{1, \dots, p-1\}$
			Compute $h_1 = g^{\alpha} \pmod{p}$
		Server hello message:	$ Compute n_1 = g \pmod{p}$
3		$hello: (p,g,h_1)$	
4	Pick a $\beta \stackrel{\$}{\leftarrow} \{1, \dots, p-1\}$	, , ,	
4	Compute $h_2 = g^{\beta} \pmod{p}$		
5		$\xrightarrow{h_2}$	
6	Compute $K = h_1^{\beta}$		Compute $K = h_2^{\alpha}$
	Change a tout man		
7	Choose a text msg having 8-10 words		
'	Compute $C = AES.Enc^{cbc}(msg, K)$		
8	Compute C = /125.Enc (msg, 11)	C	
9		7	msg' = AES.Dec(C,K)
10		msg <sup>'</sup>	<b>g</b>
10	If msg' = msg		
	output success		
11	Else		
	output fail		
12	Close the connection!!		