COSC 4343: Computer Security and Privacy

Homework # 3: due on Tue. 10/06/2020 at 11:59 pm

Remaining late days may be used in this assignment if needed.
Check "Late Days" policy in syllabus for more details.

Solve the following problems. Show your detailed work in every step of your solution.

Problem # 1:

Suppose you are to communicate securely with Alice using the RSA cryptosystem. Alice has secretly generated her own private key (N,d) = (21,5) and publicly shared her public key pair (N,e) = (21,5).

Part 1:
Generate your own public and private keys by choosing your own prime numbers p and q. For the purpose of this assignment, your prime numbers can be any value between 1 and 21, and must be different values from those used in class. Show your work.

Part 2:
Using RSA, send your actual name in the format of *"firstName lastName"* including spaces and quotations) encrypted to Alice in such a way that only Alice can decrypt the message. Show all your work. Use the table of ASCII codes at the end of this assignment to replace each character (including spaces, apostrophe, etc.) with a two-digit number for each letter.

Part 3:
Using RSA, send your actual name signature in the format of *"firstName lastName"* to Alice in such a way that anyone who intercepts the message can read and verify that you are the sender of the message. Show your work.

Part 4:
Using RSA, send your actual name signature in the format of *"firstName lastName"* to Alice in such a way that anyone who intercepts the message can verify that you are the sender of the message, but only Alice can read the contents of the message in plaintext and not others. Show your work.

Part 5:
Using RSA, send your full name to Alice in such a way that only Alice can do both (1) read the message in plaintext, and (2) verify that you are the sender of the message. Show your work.

Problem # 2 is on next page

Problem # 2:

Use Diffie-Hellman to generate a symmetric key that Alice and Bob wish to use for their secure communications. Given the generator g = 10 and the prime p = 541, Alice has chosen her private value a = 11 and Bob has chosen his private value b = 13. Compute the common symmetric key value that both Alice and BOB can compute using the Diffie-Hellman key exchange method. What does Alice send to Bob, what does Bob send to Alice? Show your work.

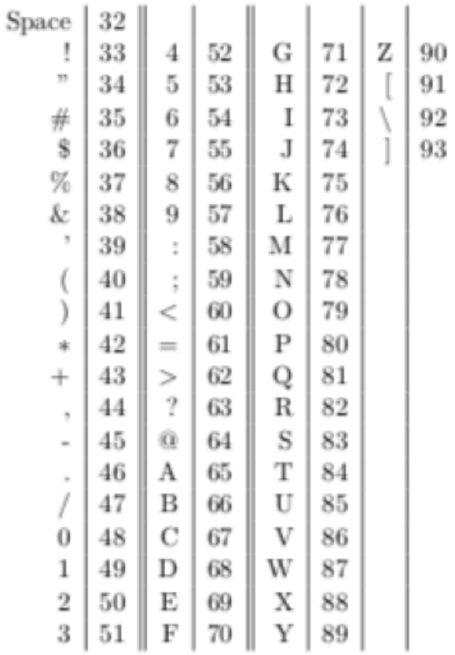
Submission instructions:

1- Your solutions should be submitted through Canvas. Email or paper submissions will not be accepted.
2- Remember that no handwritten solutions will be accepted. Please make your submission document well-formatted and look professional, with your name, course number, etc. included. Also make sure your final submission is in one .pdf document.
3- Make sure your final submission filename is of the format "HW03-*firstNameLastName*.pdf".
4- Re-download your submission and make sure it reads well as intended.

Always let me know if you have any questions or need more clarification on the assignment or submission instructions.

Good Luck ☺

ASCII codes:



Space	32						
!	33	4	52	G	71	Z	90
"	34	5	53	H	72	[	91
#	35	6	54	I	73	\	92
$	36	7	55	J	74	]	93
%	37	8	56	K	75		
&	38	9	57	L	76		
'	39	:	58	M	77		
(	40	;	59	N	78		
)	41	<	60	O	79		
*	42	=	61	P	80		
+	43	>	62	Q	81		
,	44	?	63	R	82		
-	45	@	64	S	83		
.	46	A	65	T	84		
/	47	B	66	U	85		
0	48	C	67	V	86		
1	49	D	68	W	87		
2	50	E	69	X	88		
3	51	F	70	Y	89		