SY110 Homework Alpha: ________ Name: __________________ Page 1 of 2
Collaboration Policy: Default MIDN Last, F.
choose one: □ None □ XS110 □ EI with:
(or more) □ MGSP □ Discussed with: ______________________
Homework: /SY110/Cyber Security Tools/Asymmetric Encryption

1. [15 / 10 / 5 / 0] What is the problem with setting up communication using symmetric encryption that asymmetric encryption (public-key cryptography) solves?

2. [10 / 8 / 5 / 0] Alice wants to send a message only Bob can read, so Alice encrypts her message with (circle the correct answer):

a. Bob’s Private Key b. Bob’s Public Key

c. Alice’s Private Key d. Alice’s Public Key

3. [10 / 8 / 5 / 0] Alice wants to send a message only Bob can read, and which Bob will know could only have come from Alice. So Alice first encrypts the message with ____ and then encrypts the result with _____. (Fill in the blanks from the choices below)

a. Bob’s Private Key b. Bob’s Public Key

c. Alice’s Private Key d. Alice’s Public Key

4. [20 / 15 / 10 / 0]
Bob’s public key is: `(a3f1,b65d0a1223ad294893d6663e75b02b61)`
Bob’s private key is:
`(4711eac1dafec84945f5a8613219a8a1,b65d0a1223ad294893d6663e75b02b61)`

Using `http://rona.academy.usna.edu/~sy110/resources/rsa/index2.html`, decrypt the following secret message Alice encrypted just for Bob:

```
8284eef46c161cca0dd90635811abbc38b58768a197a6e4895344206e561e3262dd1329d6f930
4f56e68f08bc31b4fbab0c886238a5065f8631d73d179119c1b48085653d052259240d11b4a73
a5c8e2a9821014bdd21ac1b48ceb9ae768ac34
```

Note: Triple click to select all of the text in an HTML Element on a web page.

Message is:

5. [20 / 15 / 10 / 0]
Alice’s public key is: `(29fc77df,a8d1d900713bebc685b1308f425e6827)`, Bob’s is the same as Question 4. Decrypt the following message, which Alice encrypted (following the scheme from the notes) so that only Bob can read it, and so that Bob knows that only someone with Alice’s private key could have sent it.

```
9ecb954d95454cc5f3139b7bcae7f7f18fae5aa0126fba90c6e8bfbf8880f0352afd3bb4d6fbd
b31ccdec93b6672b6699763917d915a551ad2116ecd37049c6b9dba34ce1b955f8cfbb331a56b
52069b4522ac902c91e3ac91f7187d8b40de3e7b5df9e682c42a55fe32210e04590f9ea145723
bf5f2d7b02f6f9ec9595935a8af8fd4149f6c59441b90a6ddc78bf7fa45a4f31113a9eb53fcbb
940902df5ac0ab563da17df9a86b718197569cc0ae77892c07ee5c8c30420867c406d6b502b45
8430a61f13a11b0c5ab6362fbf334ae1f1f9ddb981b427756801ce5d8c5e9c182049fc0e49f68
a37a1aa346109a6d079caf7b7ce5a39d9f32895090b05ffdbd8a3a916d7f70c330f5c59e421d6
144f60312193dfeab1c5b4ca65b93c184ea6d69b76bb321a18f76060e385300f8d8e0a006a0e4
8dd76aaf05060d73ed3d2d387152dff95dba2460c31bec70db12251c
```

Message is:

6. [10 / 8 / 5 / 0]Explain how we know that the message in Question 5 had to come from someone that has access to Alice’s private key?

7. [15 / 10 / 5 / 0] What Pillar of Cyber Security are encryption schemes, symmetric and asymmetric, in general designed to provide?