

1. You are Alice. If you need to have a private chat with Bob and a separate private chat with Carroll, will you use the same public key to secure both conversations? Why?

2. How many total keys are required for two parties to communicate via asymmetric encryption?

3. A) Which requirements of the 5 Pillars of Information Assurance are met by the following techniques:

Encryption	C	I	A	N	A
Symmetric					
Asymmetric					

B) How so?

4. Circle the correct choice.

A) **Symmetric / Asymmetric** encryption is faster and more efficient.

B) **Symmetric / Asymmetric** encryption is easier to manage and deploy on a large scale.

5. What mathematical assumption is the RSA algorithm based upon?

6. Follow the reading link on the syllabus for today. It should take you to an SI110 page which has an RSA demo halfway down the page. Bob has encrypted the following message for Alice (Input).

11716791e0e899217083a51cfb8e927e05e80a22a66bafd08be5007d301274970ee983733bfc93af5a4be9ed1a5d1d50d3b5de72a7b270c69035cc9a35913d713a358076052c8b4486a1528dacc2e6d

What does it say?