CSC 6222 Assignment 1

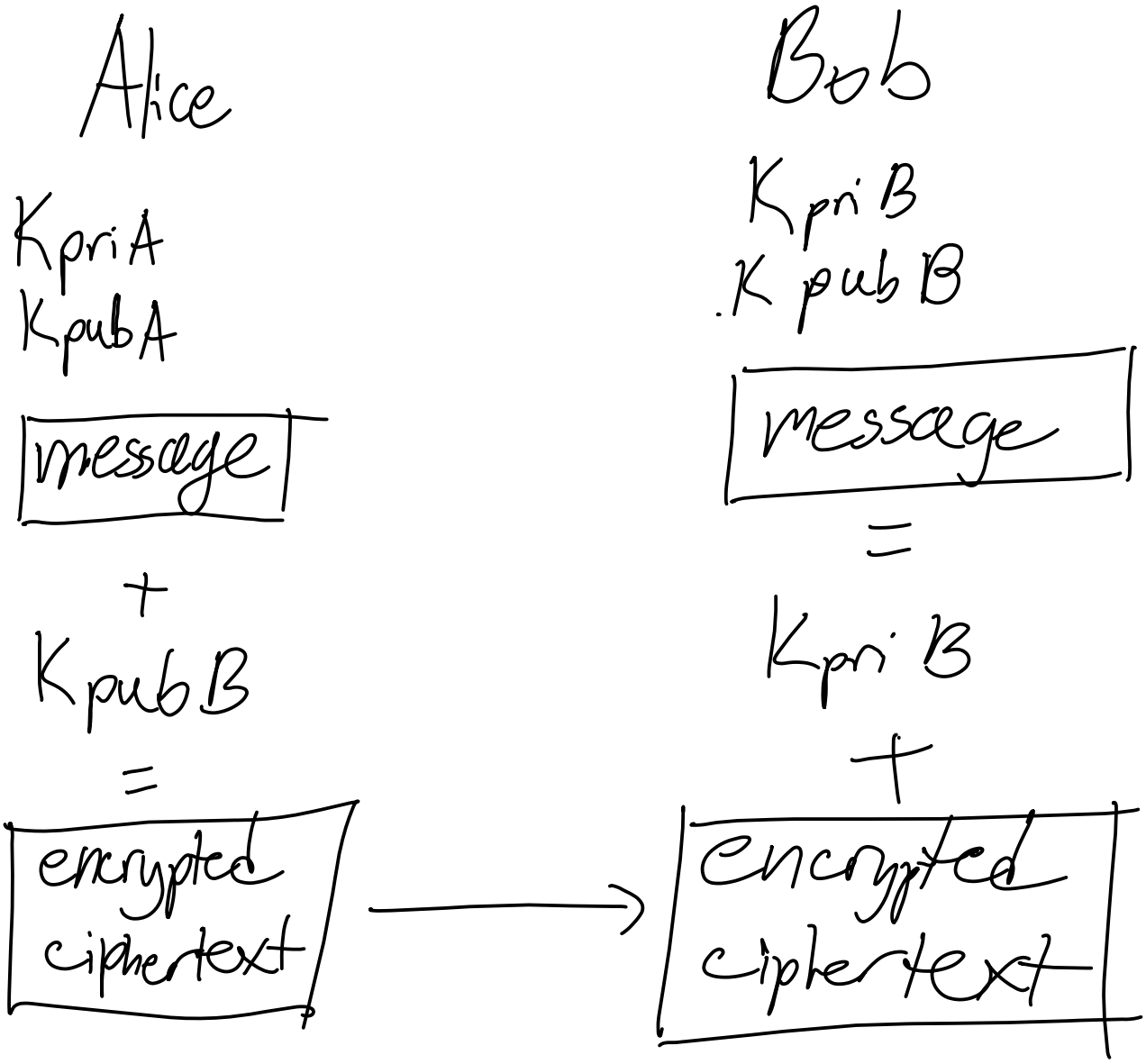
1.
    a. C.I.A. stands for Confidentiality, Integrity, and Availability. These three concepts represent the basis of security for both computers and personnel. Tools to achieve each of the concepts in C.I.A. include encryption, logging, access control, authorization, and authentication.
    b. Confidentiality refers to an adversary cannot find out who sent the message or to whom it will reach. Integrity refers to the adversary not being able to change the message without it having noticeable effect. You can have confidentiality without integrity by sending a message that when tampered with will just be lost and losing only integrity. You can have integrity without confidentiality by sending a cleartext message that will show signs if it is tampered with.
    c.
        i. Confidentiality, Authenticity
        ii. Availability
        iii. Integrity, Availability
        iv. Integrity, Authenticity
        v. Authenticity, Availability
        vi. Availability, Integrity, Authenticity
        vii. Availability, Confidentiality, Authenticity
        viii. Availability
        ix. Availability, Authenticity

2. Symmetric encryption is usually faster to execute, simpler to create algorithms for, and is used in near real time scenarios. However, public key encryption uses fewer keys, uses separate keys for encryption and decryption, and is generally slower than symmetric encryption.
3. Authenticity means verifying the message was sent by a particular sender. Signatures, error check codes, and checksums are the tools to verify authenticity. Bob cannot violate an agreement of his own digital signature since the signature was created with his key and message, therefore verifying he is the sender and the message was made by him.
4.
    a. Changing the message or data sent in order to make it unusable or invalid. Protection: add redundant data in the form of a checksum
    b. An attack on availability. Denying services to users trying to access resources. Protection: setup redundant services or mask the source or destination of the data.
    c. An attack on confidentiality. Links data to a particular person, place, or event. Protection: ensure randomness of data to prevent potential linking of data to any particular user.
5.

a. A system without fail-safe defaults will have every user access to all functions of the system and could promote malicious or unintentional changes at critical parts of the system.
b. The system would allow for users to access resources that aren't in complaint with a protection scheme, therefore allowing certain resources some users shouldn't have access to.
c. The system would allow anyone access as long as they passed a singular point of entry rather than accomplishing multiple conditions to gain entry.

6.

a. No, without a public key that Alice can use to create her own signature she cannot send a message that can be verified by Bob with the hash function.
b.



7.
    a. You cannot directly reverse a hash of a message since it is a one way function. You will need additional data such as a dictionary or some other list of words to see what hash represents.
    b. Since public key encryption is more computationally expensive, it makes sense to compute a small message digest of small size rather than encrypting an entire message in order to provide integrity.
8. Salting with a userid introduces new risks that would not happen if just using a random value each time for a salt for every user. Lets say there are only 26 lowercase letters that can be used for the 6 character userid and password. That means each username and password has 26^6 or 308,915,776 possibilities. Using a random salt value, the hacker would have to create a rainbow table with 26^6 userid and 26^6 password hash combinations and *then* also deal with the random salt value. Without a random salt value and instead using the userid hash as the salt, then the hacker just has the 26^6 userid and 26^6 password combinations since he or she has already calculated the salt by calculating the hashes of the userid. This *significantly* changes the amount of time it takes to crack an account userid and password which, depending on the algorithm hash used, would make cracking the trivial.
9. 128^8 potential passwords or 7.2057594e+16 possibilities. 128^8 possibilities x 10^{-9} seconds x ½ time on average makes for 36,028,797.01894 seconds or about 417 days.
10.
    a. Barack should attach a signature to his message by using a hash algorithm and private key to attach to his message. That way, anyone can decrypt the signature with the same hash algorithm and Barack's public key and comparing it Barack's message to know that Barack sent the message and no one else.
    b. Yes, since if Bill tries to intercept the message he cannot change it since he does not have the key that Hillary and Barack have shared together. As long as the key is not compromised, Hillary can be sure the message was sent by Barack.