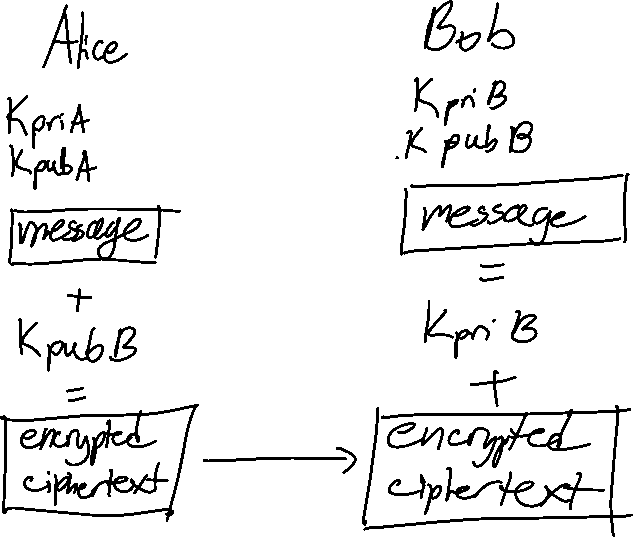
HW2

1. 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.
2. A non-forgeable, verifiable document requires that the signature require some near-impossible task that the other party can use a process to see if it is genuine. In the past, special inks and codes were used to protect documents, but now digital signatures are used. Digital signatures use a one-way hashing encryption algorithm that is near-impossible to forge and a low compute time, decryption algorithm that can be used to verify the message bits that matches the signature of the party sending it.
3. 1. 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.



1. 1. You would need sequence numbers in order to send the correct NACK to the sender to make sure that particular data is sent again.
   2. The receiver would need a timer to make sure the sender didn’t send the data and the NACK needed to be sent again.
   3. The sender would send a packet of data to the receiver with a unique sequence number. The receiver would only send a NACK if it received a packet with an unexpected sequence number. The receiver would set a timer for the NACKs and resend when it times out. The NACK-only protocol would fail in flow control since the receiver never sends a message to the sender if it is overloaded.