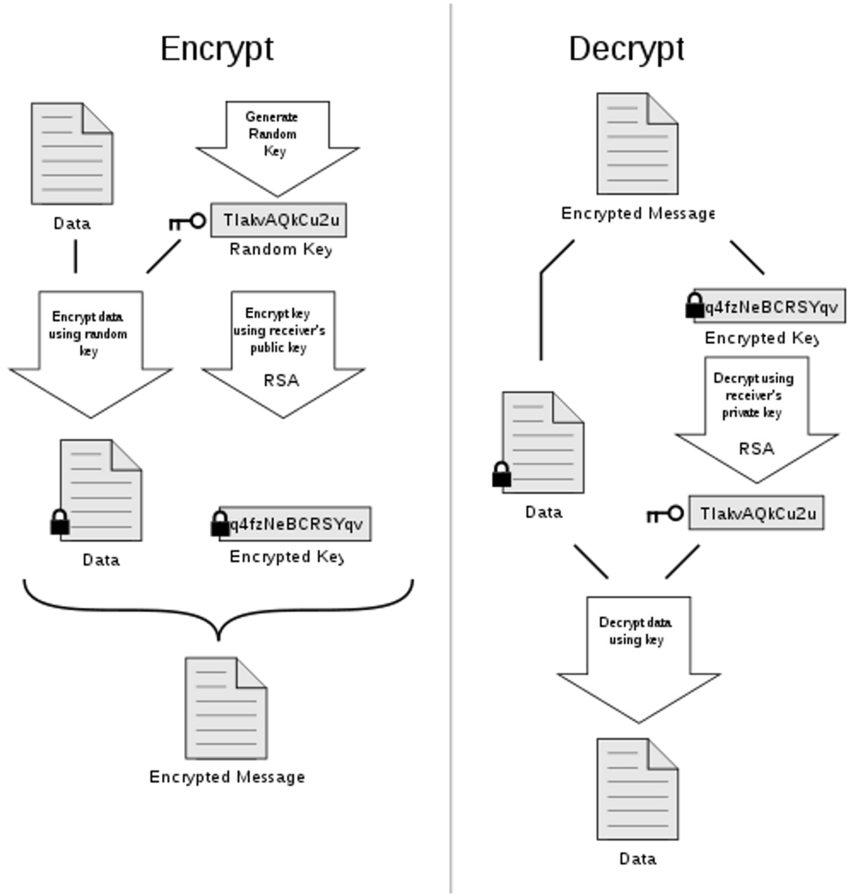
Computer Security and Privacy (COM-301)

Applied cryptography II

Interactive Exercises

PGP

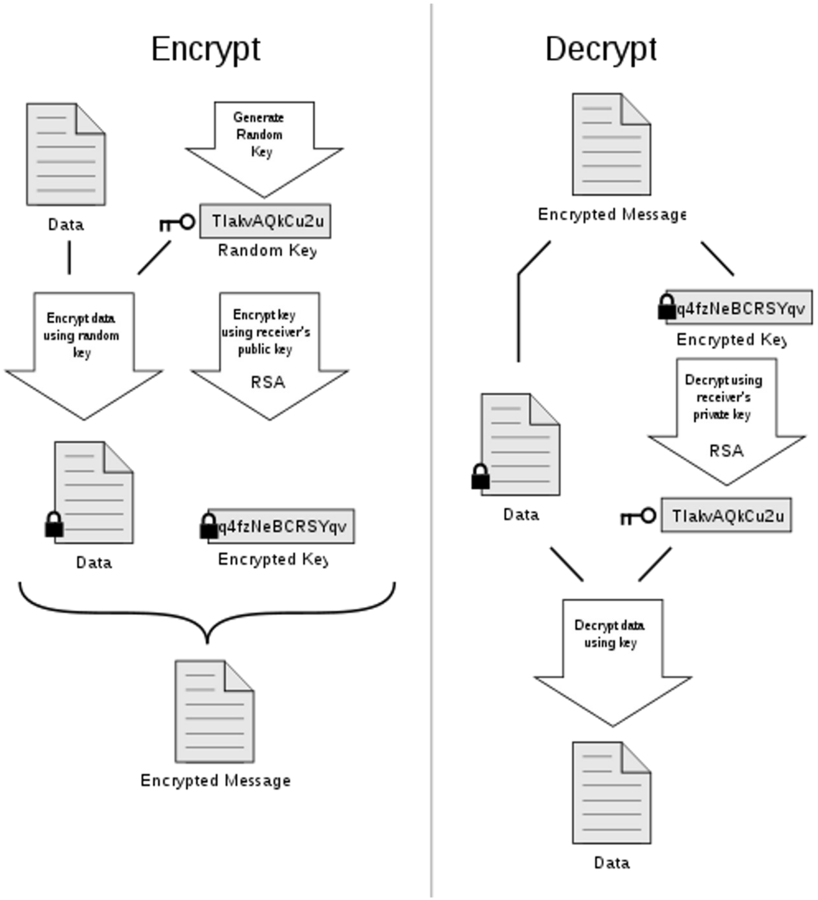
The following picture explains how PGP (Pretty Good Privacy) used to encrypt emails.



(a) Why does this scheme provide confidentiality?

PGP

(b) If you want the scheme to also provide integrity of the message, what would you add?



PGP

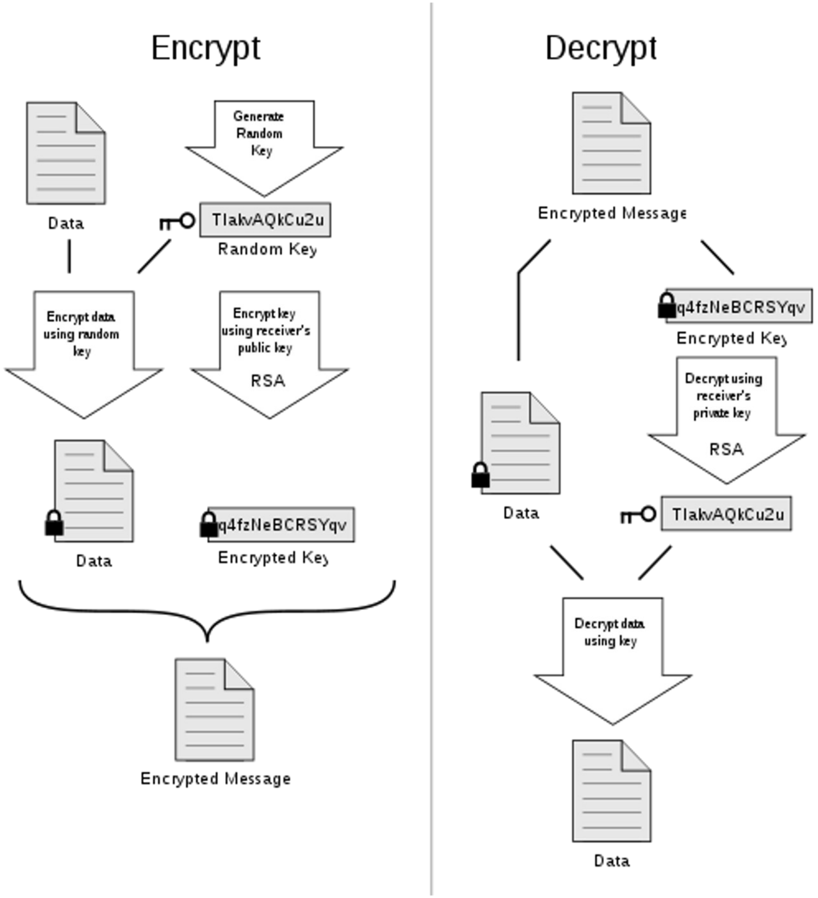
(b) If you want the scheme to also provide integrity of the message, what would you add?

Option 1: Add a hash of the message

`Enc(k, data||H(data)), Enc(PKrec, k)`

Option 2: Add a signature of the data and the key

`Enc(k, data), Enc (PKrec,k), Sig(SKsen,data||k)`



`Enc(k, m)` - Encryption of message m with key k

`H` – Cryptographic hash function

`Sig(k, m)` - Signature of message m with key k

`PKrec` – Public key of the receiver

`SKsen` – Secret key of the sender

Destination Fakeland

A group of security researchers traveling to Fakeland learn that, upon arrival at the airport, Fakeland's border authorities will require their laptops for inspection. Fakeland authorities are famous for installing spying software during the inspection, so the researchers decide to take a snapshot of the laptops' state to make sure that they can detect changes.
For this purpose they plan to hash the content of the laptops' hard drive and write this hash on a paper. This way when they receive their laptops back, they can compute the hash of the content again and compare it to the value in their notes.

What property or properties must the hash function have in order to prove that no new software was installed (by comparing the hash on the piece of paper with the hash computed after crossing the border)? (Justify your answer)

Geletram

Alice uses the Geletram application to send messages to Bob. Alice and Bob share a secret symmetric key K. This key K is also known by Geletram.
For each message msg Alice wants to send to Bob through Geletram, Geletram does the following:

It generates a fresh symmetric key KGeletram, it sends
packet = {c = Encrypt(K, msg), m = MAC(KGeletram, c), KGeletram}
to Bob's Geletram to be decoded, where Encrypt is a symmetric encryption scheme, and MAC stands for Message Authentication Code.

Eve is an adversary that controls the channel in between Alice's Geletram and Bob's, i.e., Eve can read and modify any packet before it reaches Bob's Geletram.

Does Geletram provide confidentiality and integrity of the message msg with respect to Eve? Justify.