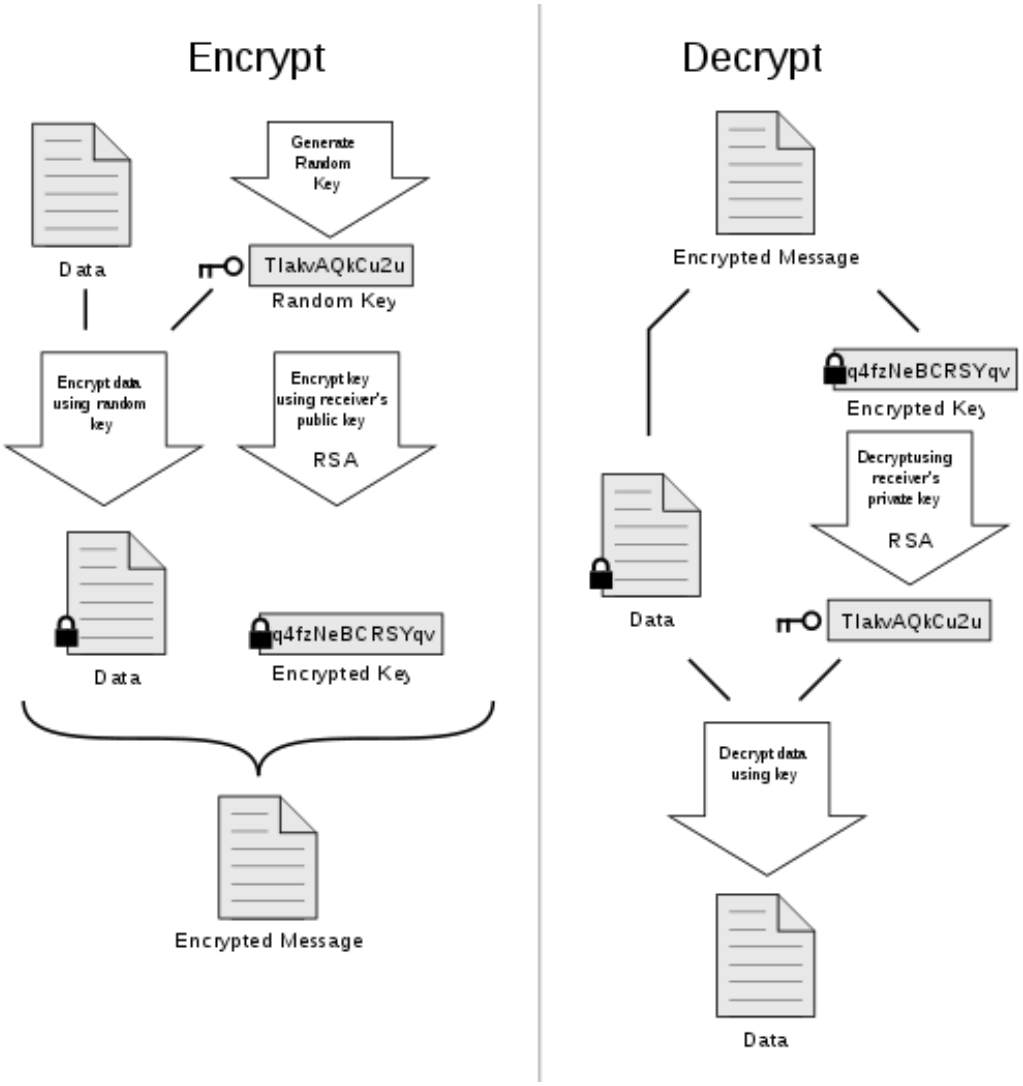
Zadatak za vežbu – PGP

PGP predstavlja program za šifrovanje, kreiran od strane Fila Cimermana 1991. godine. Koristi se za šifrovanje e-mail-ova, datoteka, direktorijuma, kao i particija samog diska. Na osnovu njega je nastao I danas najpopularniji standard za šifrovanje e-mail-ova, OpenPGP. Gruba skica algoritma je prikazana na sledećoj slici:



Zadatak na ovom, i narednih nekoliko termina će biti realizovati program koji funkcioniše po sličnom mehanizmu. U prvoj fazi, algoritam opisan u narednim koracima treba realizovati pomoću DES algoritma, i ECB moda, i prodiskutovati nedostatke. Uraditi zadatak po sledećim tačkama:

1) Izvršiti kompresiju subject i text dela unetog mail-a. (Pogledati klasu GzipUtil)
2) U klasi WriteMailClient izvršiti enkripciju simetričnim algoritmom subject i text dela mail-a pre samog slanja. (Pogledati klasu SymmetricDES projekta Crypto)
3) Nakon enkripcije, izvršiti snimanje ključa u folder data, fajl session.key. (JavaUtil klasa sadrži metodu za pisanje bajtova (*writeBytes*))
4) Nakon toga, izvršiti preuzimanje prethodno snimljenog ključa u klasi ReadMailClient. Radi ovoga, pogledati SealedObjectExample klasu projekta Crypto.
5) Izvršiti dekripciju subject I text dela maila u okviru klase ReadMailClient. Pogledati klasu SymmetricDES projekta Crypto.

6) Izvršiti dekompresiju dekriptovanog subject I text dela odabranog mail-a.

Nakon što su uspešno realizovane prethodne tačke, modifikovati zadatak tako da se koristi AES algoritam, u CBC modu, sa različitim inicijalizacionim vektorima za svaku enkripciju. Pogledati klasu SymmetricAES. Preuzimanje ključa za AES iz binarnog fajla je moguće uraditi na sledeći način:

```
SecretKey secretKey = new SecretKeySpec(JavaUtils.getBytesFromFile(KEY_FILE), "AES");
```

Ostatak protokola će se implementirati na nekom od narednih termina vežbi.