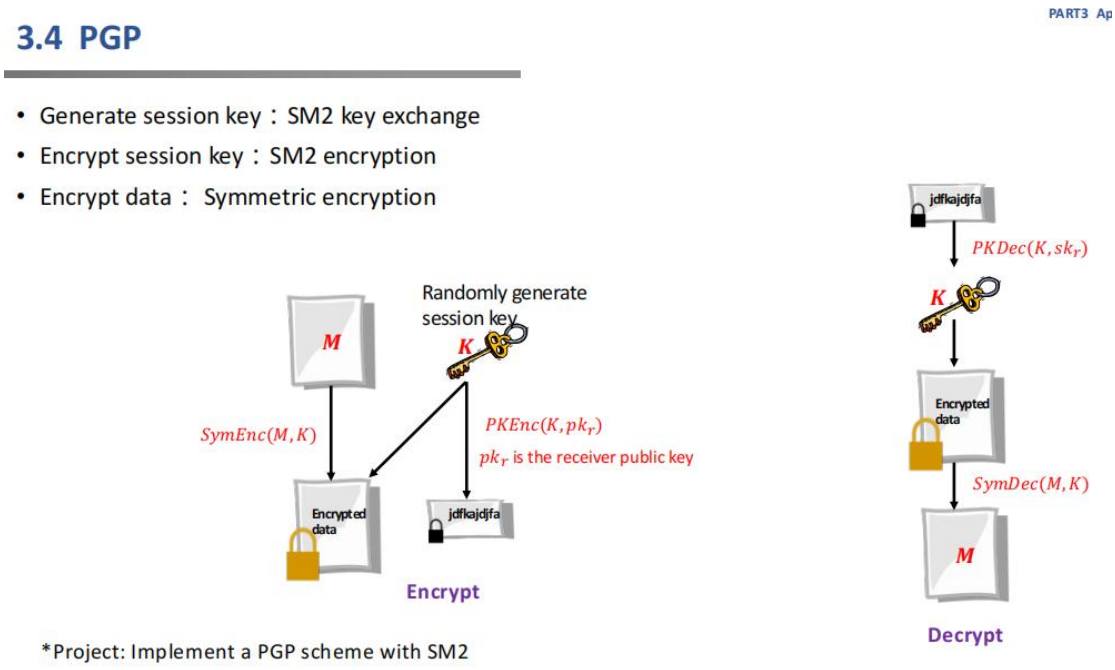
*Project14: Implement a PGP scheme with SM2

说明：

此项目是利用 SM2 实现 PGP。



首先发送者和接收者分别生成 SM2 的公钥和私钥，并进行密钥交换。

发送者基本步骤如下：

（1）随机生成临时会话密钥 K（对称加密的密钥），本项目对称加密使用的为 AES。

（2）用 K 对要发送的消息进行 AES 加密得到 a。

（3）用 SM2 的公钥加密 K 得到 b。

（4）对 K 进行签名，便于接收者验证得到 s。

（5）把 a、b、s 发给接收者。

接收者基本步骤如下：

（1）用 SM2 私钥解密 b 得到 K。

（2）验证签名。

（3）用 K 进行 AES 解密得到发送者发的消息 m。

为了本次项目实现方便，把发送者、接收者写在了一个文件里，重要代码如下：

```
#开始
print("##############发送者部分################")
m="202100150084"
print("要发送的消息：")
print(m)
k = K_random(16)    #随机生成一个AES加密的密钥
print("随机生成的AES加密的密钥为：")
print(k.encode('utf8'))
a=AES_enc(m,k)      #用对称加密AES加密消息m
b=sm2_enc(k.encode('utf8'))     #用sm2加密AES的密钥k
s=sign(k.encode('utf8'))     #签名，用于接收者验证
print("发送成功")    #把a,b,s发送给接收者

print("##############接收者部分################")
key=sm2_dec(b)     #解密sm2得到AES密钥
print("接收到的AES加密的密钥为：")
print(key)
p=sm2_ver(s,key)  #验证签名，确定AES密钥的正确性
if p:
    m=AES_dec(a,key.decode('utf8'))  #如果AES密钥正确，用其解密AES得到消息m
    print("接收成功，消息为：")
    print(m)
```

实现方式：python

效果：在自己电脑上 CPU：11 代 i7

```
============================ RESTART: E:/project14.py ==
##############发送者部分################
要发送的消息：
202100150084
随机生成的AES加密的密钥为：
b'fhSfgronjzaJUuhr'
发送成功
##############接收者部分################
接收到的AES加密的密钥为：
b'fhSfgronjzaJUuhr'
接收成功，消息为：
202100150084
```

分工：自己独立完成