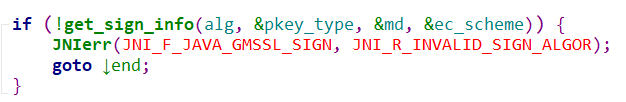
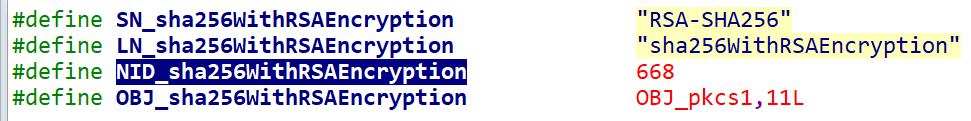
1. Alg = “RSA-SHA256”



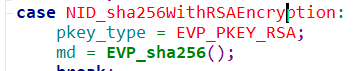


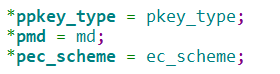


int pkey\_type;

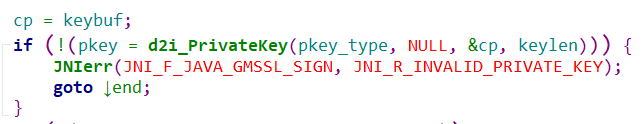
const EVP\_MD \*md = NULL;

int ec\_scheme = -1;



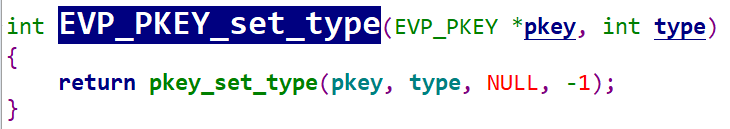


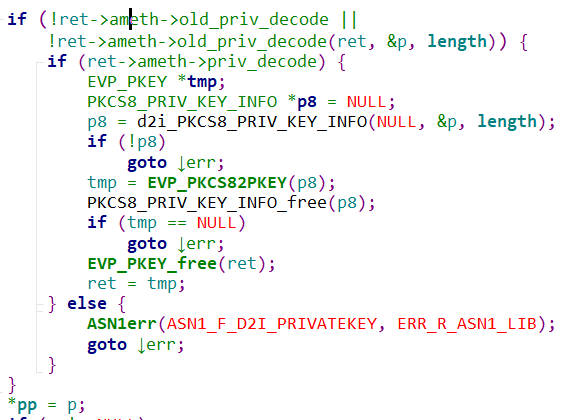
1. keybuf

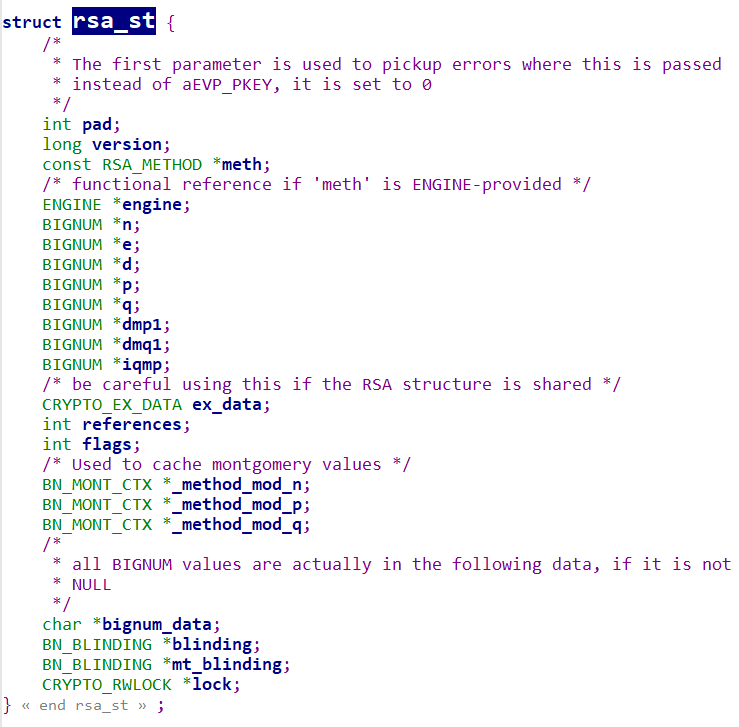


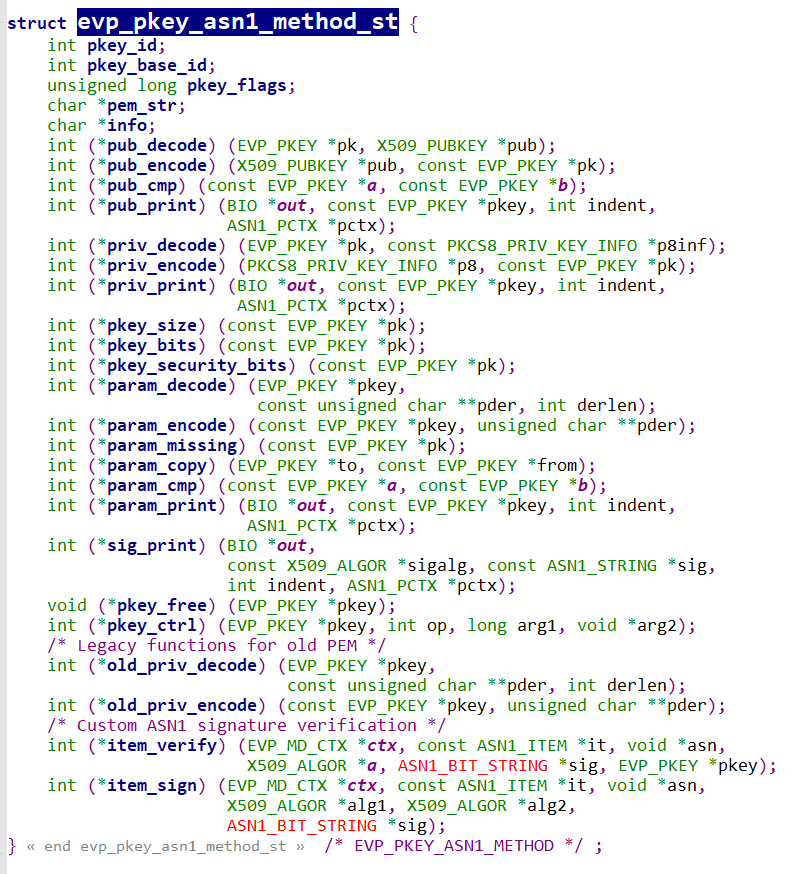
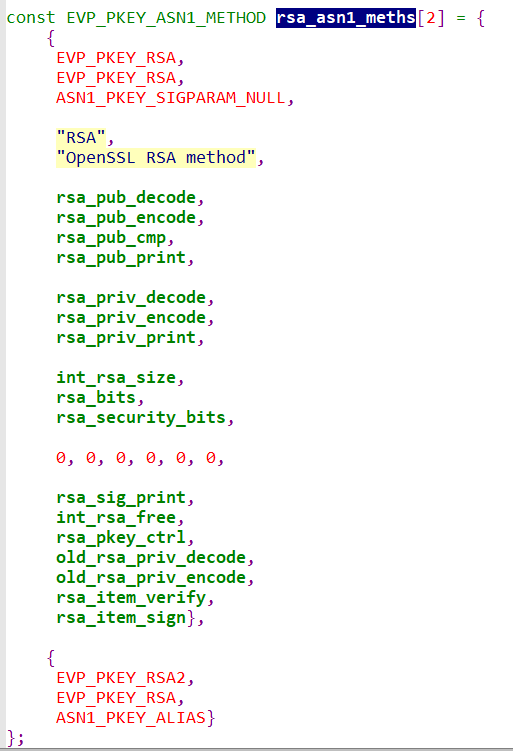
ret = EVP\_PKEY\_new()

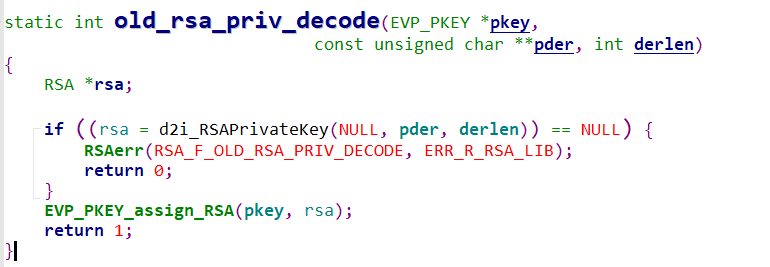
EVP\_PKEY\_set\_type(ret, type)



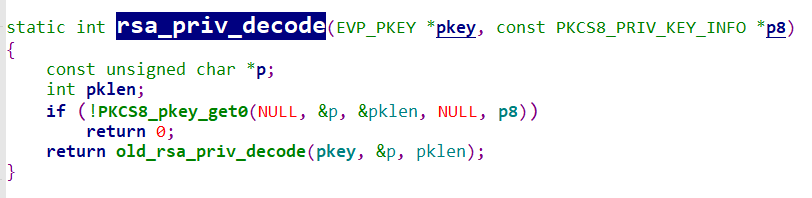


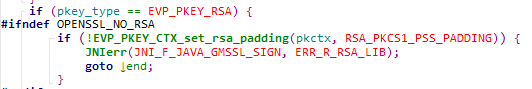




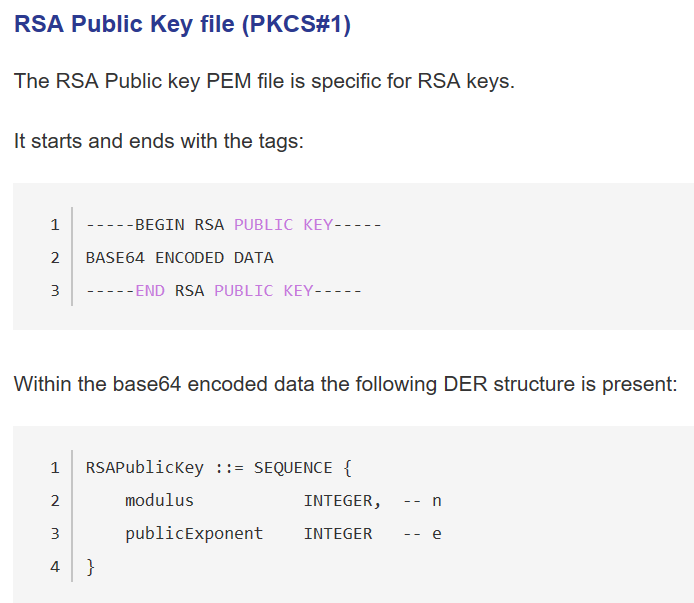


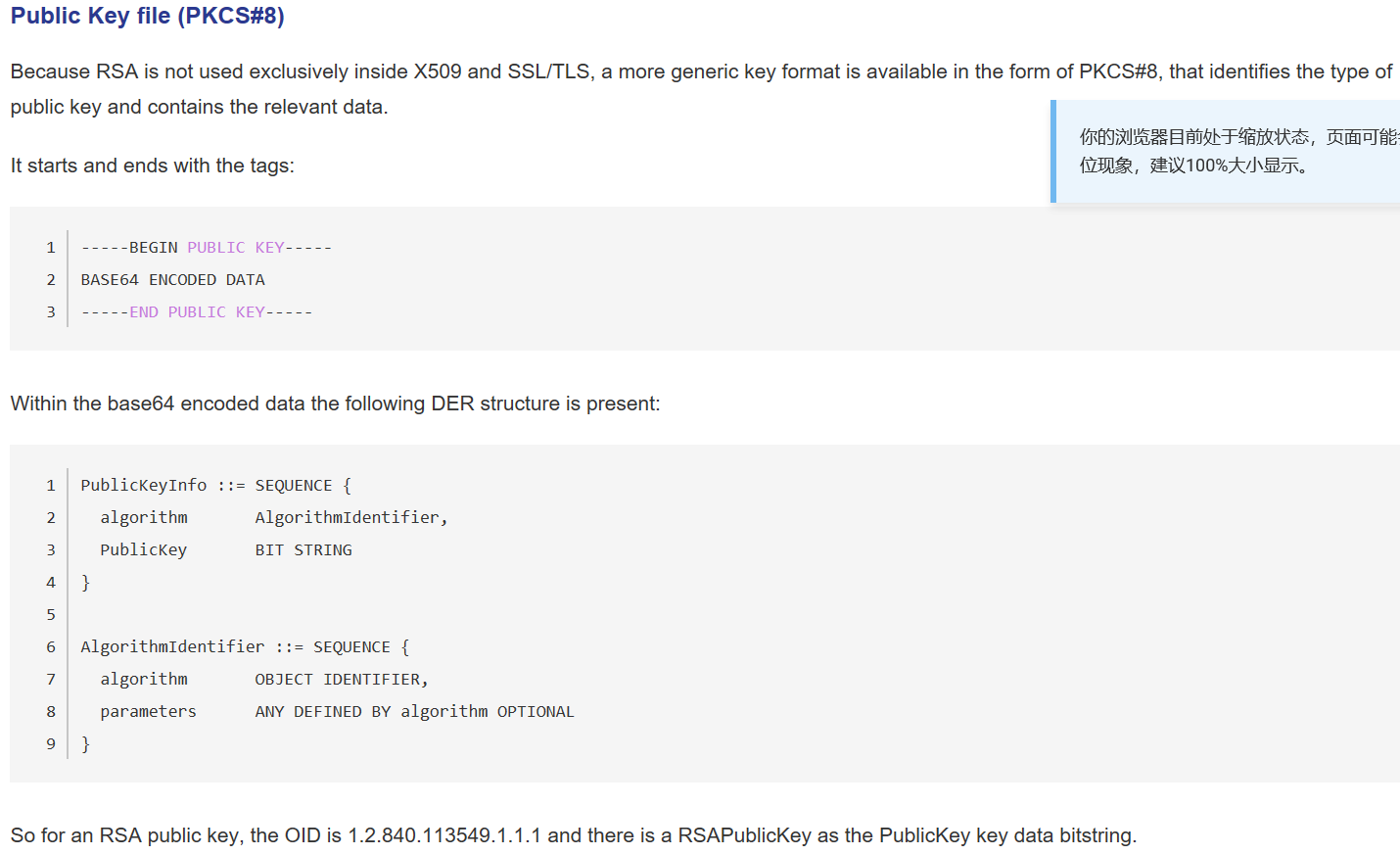
*d2i\_RSAPrivateKey()*, *i2d\_RSAPrivateKey()* decode and encode a PKCS#1 RSAPrivateKey structure.



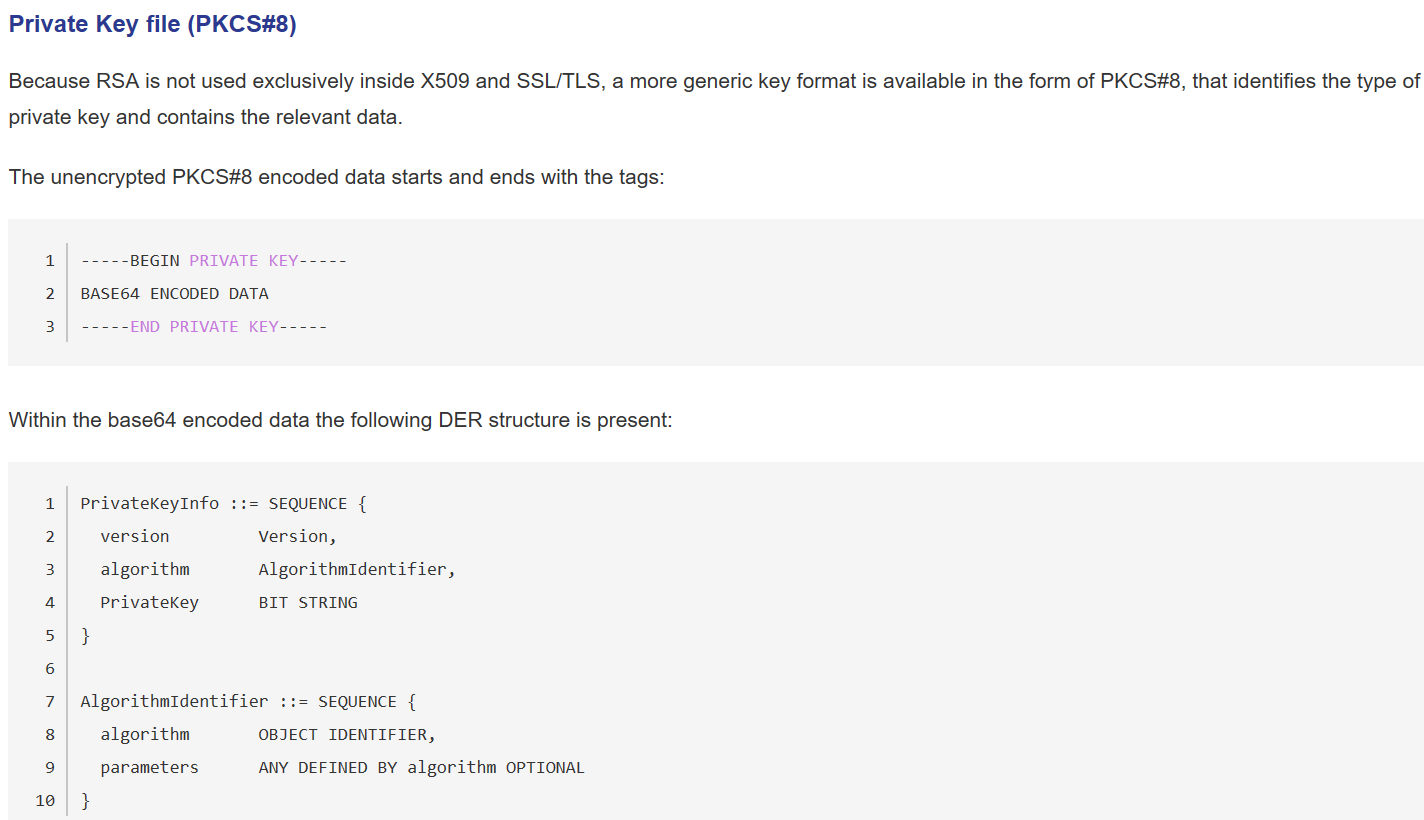


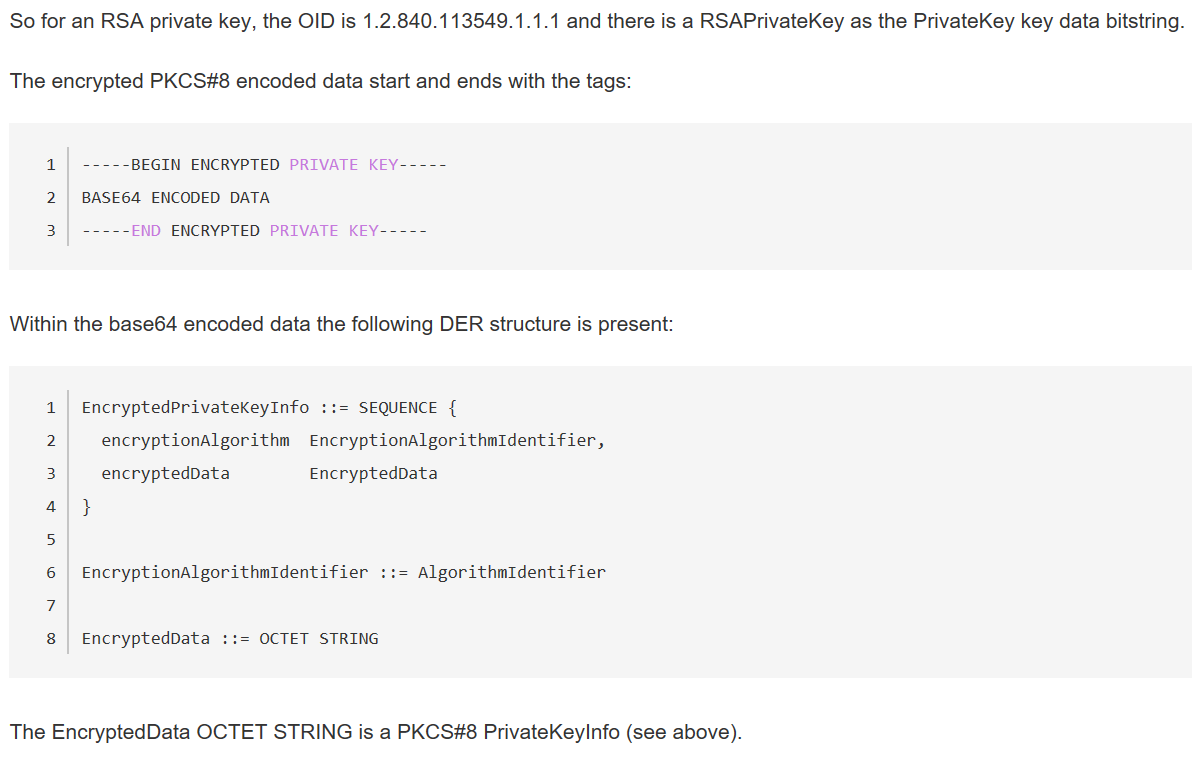
## PKCS1 vs PKCS8











pkcs\_pri

privateKey

pkcs\_pub

d

n

e: 010001