

Expectations for second cryptography exam Tuesday December 6 at 1:30. Bring a calculator and blank sheets.

I will hold office hours 4:30 - 5:30 on Monday and 12:20 - 1:20 on Tuesday of finals week. The following will be at the top of your exam:

a=0,b=1,c=2,d=3,e=4,f=5,g=6,h=7,i=8,j=9,k=10,l=11,m=12,n=13,o=14,p=15,q=16,
r=17,s=18,t=19,u=20,v=21,w=22,x=23,y=24,z=25
 $r = g^k(\text{mod } p)$, $S = aAr + kx(\text{mod } p - 1)$, $g^S = (g^{aA})^r r^x(\text{mod } p)$.

Also at the top will be as much as you need to know for key expansion, encryption or decryption (whichever I ask you for) with simplified AES. There will also be an ASCII table, if needed.

Expectations: Know Playfair; AFDGVX; encryption/decryption with $C \equiv aP + b(\text{mod } N)$; encrypt/decrypt/key expand for simplified AES; use repeated squares algorithm; understand public key cryptography: its uses, how it differs from symmetric key cryptography; use RSA for encryption/decryption/signing; know what is the FFDLP and ECDLP and how they differ; use FFDH, ECDH; FF- and EC- ElGamal Message exchange, Massey-Omura; ElGamal signatures; how to add and double points on an elliptic curve using line intersections; know purposes and properties of hash functions and MACs; know how certificates are used and the cryptographic entries in them; know what is sent back and forth in SSL (though you need not memorize the order of the steps).

You may ask yourself how on earth you can do an ECDH or EC-ElGamal without PARI. Trust me - I can make it work with little effort on your part.