FOUNDATIONS OF CRYPTOLOGY

ASSIGNMENT 5

Problem 1

Alice published the following RSA public key:

N :=

29905476219696696488459695569542874982899982395591783167345616213742428520932979864701105762419

e := 13223141

Bob sent a message to Alice, encrypted using this key. The encrypted message is:

E :=

184708672366520421146742024126723615082869226247989540474628481415946044811051997720443185680 85

Alice's private key is:

d :=

29101241661082444091235600206473561533438079973101886056474137926863097442817516466883649517741

Determine the content of the message.

Answer 'Trouble in Kenya!'

Problem 2

Alice and Carol have the same RSA encryption modulus:

N :=

29905476219696696488459695569542874982899982395591783167345616213742428520932979864701105762419,

but have different encryption exponents.

Alice's encryption exponent is eA:= 257982598332521, and

Carol's encryption exponent is eC := 8357598759827897559827.

Bob sent the exact same message to both Alice and Carol, encrypted with their respective public keys. The encrypted messages are as follows:

(a) The encrypted message for Alice:

EncrA:=

25742211972573775074584023844806862826724677794637841736155082773353826650560036988594385927380

(b) The encrypted message for Carol:

EncrC:=

11021170567433275103287488918357139494535033415363428500376802294402114235404106032323041033864

Bob tells Dave that he sent the same message to all of his female friends, but didn't tell Dave what the message was. Dave, envious of Bob's relationships, constantly eavesdrop on Bob's communication with others. Dave sees EncrC and EncrA. Show that Dave can decrypt the message.

Answer 'How about a date?'