

Homework 11, due October 13

- (1) (a) Find a primitive root modulo 97.
(b) (Page 108, problem 26) Let $p \equiv 3 \pmod{4}$ be prime. Show that $x^2 \equiv -1 \pmod{p}$ has no solutions. (Hint: Suppose x exists. Raise both sides to some power and find a contradiction.)
- (2) Your public key is $e = 17$. You know that the factors of n are

78032062222085722974121768604305613921737282772729

and

95310075487163797179490457039169594160085543772343.

You receive the following message.

3780959489067185927636742897782124526407151622687008317493719218153002463614275880066047374967868051

Decrypt.

- (3) Suppose that $p = 14537036194383598514849719$, $q = 1535321421800476758846347$, and $e = 457$. The ciphertext $c \equiv m^e \pmod{pq}$ is transmitted, but an error occurs during transmission and the last digit is dropped. The received ciphertext is

1488700004428137646452763830564973224679560374573

Determine the missing digit and decrypt the message.

- (4) Bob creates an RSA cryptosystem with public key (n, e) given by
(20491856230948562019834234623657345734012602330942702908732328649949694281671722592058359029473,
7542635147686360696378876546501156037139772222001304920419631).

Alice sends messages to Bob by representing each alphabetic character as an integer between 0 and 26 (A corresponds to 1, B to 2, etc., and a space to 0), and then encrypting each number separately using Bob's RSA cryptosystem. Eve intercepts the following message.

5587597796128227623604187941176536495007175313370370324086855097073328273123327984102915100450017,
19936165476955767975388753129354769465931281124972425921019908374422748378862407110093671126296434,
0,

16116114783782618319770959152745233489481901622669232003113196000471601664485355429028506659785513,
11173852285322115230950985205469798146978264894498902489260450057327571287100728615800987750907326,
5587597796128227623604187941176536495007175313370370324086855097073328273123327984102915100450017,
19936165476955767975388753129354769465931281124972425921019908374422748378862407110093671126296434,
0,

19936165476955767975388753129354769465931281124972425921019908374422748378862407110093671126296434,
11215461433626929276590656885567886265220628997448555510198394409221362052776388361833442361775596,
10278303802353403640105331578831100464134331245109281004354098140786099655253977200951075546333712,
10368376228532808210943700080630088600339813360750587902850349679157627498037268910416389880192688,
3557997707330576969697469454799560750281845272775625755385466961636478070504596120602614131016531,
11215461433626929276590656885567886265220628997448555510198394409221362052776388361833442361775596

Decrypt, without factoring n .

Subsequently, Alice realizes the error of her ways and sends Bob a new message using his RSA public key. Her message is

1484238733694463376886546869753096084758497375154174768539576555246062116158890795115972577981497.

Decrypt. Answer Alice's question. (Use plaintext.)