Homework 16, due October 12

(1) Your public key is $e = 17$. You know that the factors of n are

$$780320622220857229741217686043056139217372827729$$

and

$$9531007548716379717949045703916959416008554377234 3.$$

You receive the following message.

37809594890671859276367428977821245264071516226870083174937192181530024636142758800660473749678680 51

Decrypt.

(2) Suppose that $p = 14537036194383598514849719$, $q = 15353214218004767588463 47$, 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

148870000442813764645276383056497322467956037457 3

Determine the missing digit and decrypt the message.

(3) Bob creates an RSA cryptosystem with public key (n, e) given by

(20491856230948562019834234623623657345734012602330942702908732328649949694281671722592058359029473,
75426351476863606963788765465011560371397722220013049204196 31).

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.

558759779612822762360418794117653649500717531337037032408685509707332827312332798410291510045001 7,
199361654769557679753887531293547694659312811249724259210199083744227483788624071100936711262964 34,
0,
161161147837826183197709591527452334894819016226692320031131960004716016644853554290285066597855 13,
111738522853221152309509852054697981469782648944989024892604500573275712871007286158009877509073 26,
558759779612822762360418794117653649500717531337037032408685509707332827312332798410291510045001 7,
199361654769557679753887531293547694659312811249724259210199083744227483788624071100936711262964 34,
0,
199361654769557679753887531293547694659312811249724259210199083744227483788624071100936711262964 34,
112154614336269292765906568855678862652206289974485555101983944092213620527763883618334423617755 96,
102783038023534036401053315788311004641343312451092810043540981407860996552539772009510755463337 12,
103683762285328082109437000806300886003398133607505879028503496791576274980372689104163898801926 88,
355799770733057696969746945479956075028184527277562575538546696163647807050459612060261413101653 1,
112154614336269292765906568855678862652206289974485555101983944092213620527763883618334423617755 96

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

148423873369446337688654686975309608475849737515417476853957655524606211615889079511597257798149 7.

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