Reading: Barr, §4.6

Exercises: Write your solutions clearly, remembering that they will be graded for presentation as well as correctness.

A1. Eve decides she wants to read Alice's mail, so she goes to the RSA public-key directory and finds Alice's keys, m_{ALICE} and e_{ALICE}. In order to find Alice's decryption key, Eve will have to factor m_{ALICE}, which is assumed to be the product of two primes.

Eve knows only one way to factor a number m: she tries dividing m by all the primes less than or equal to $\sqrt{m}$. Her computer can complete 100,000 of these trial divisions every second.

(a) Supppose that m_{ALICE} is approximately 3×10^{19} (that is, it's a twenty-digit number starting with 3). Approximately how long would it take Eve's computer to divide m_{ALICE} by all the primes up to $\sqrt{m_{\text{ALICE}}}$?

(b) Suppose Eve's computer program picks the trial divisors in a random order. Then she might get lucky and hit on one of the factors of m_{ALICE} right away. What is the probability that Eve's very first guess is one of the factors of m_{ALICE}?

(c) Now suppose $m_{\text{ALICE}} \approx 3 \times 10^{39}$ (that is, she uses a forty-digit number). How long will Eve's computer take to check all the possible prime divisors?

(d) How long will Eve's computer program take if $m_{\text{ALICE}} \approx 3 \times 10^{59}$?

A2. As we've seen in class, the number of digits in n_{ALICE} is usually the same as the number of digits in m_{ALICE}. When Alice uses a twenty-digit value for m_{ALICE}, it takes her computer about 1 second to run the extended Euclidean algorithm and find the value of d corresponding to any given e.

Alice is worried about security, and switches to a forty-digit value for m_{ALICE}. Based on your experience with the extended Euclidean algorithm, how long will it take Alice's computer to find the value of d corresponding to any given e?

How long will it take if m_{ALICE} has sixty digits?

Here's a page from the Factorville RSA Key Directory:

e_{ALICE}	=	34153	m_{ALICE}	=	243569
e_{BOB}	=	42713	m_{BOB}	=	339551
e_{CARL}	=	292811	m_{CARL}	=	321401

B1. (a) Alice receives four plaintext messages, each one with a digital signature attached. The plaintexts are 2003, 2004, 2005, and 2006. The complete, signed messages are

$$(2003, 116851), \quad (2004, 219536), \quad (2005, 288864), \quad (2006, 162131)$$

Each of the messages is either signed by Bob, signed by Carl, or is a forgery. Which is which?

(b) Suppose the forgery in B1a was actually a message from Bob that was intercepted and altered by Eve. What was Bob's intended message?

B2. Eve, who spends all her time trying to defeat cryptographers, determines that m_{ALICE} is the product of the primes 373 and 653. She decides to impersonate Alice, by sending the message 1992 to Bob, with Alice's signature on it.

(a) What signature should Eve affix to the message 1992 in order to pretend to be Alice?

(b) Eve encrypts her signed message using Bob's public key. What numbers does she send to Bob?