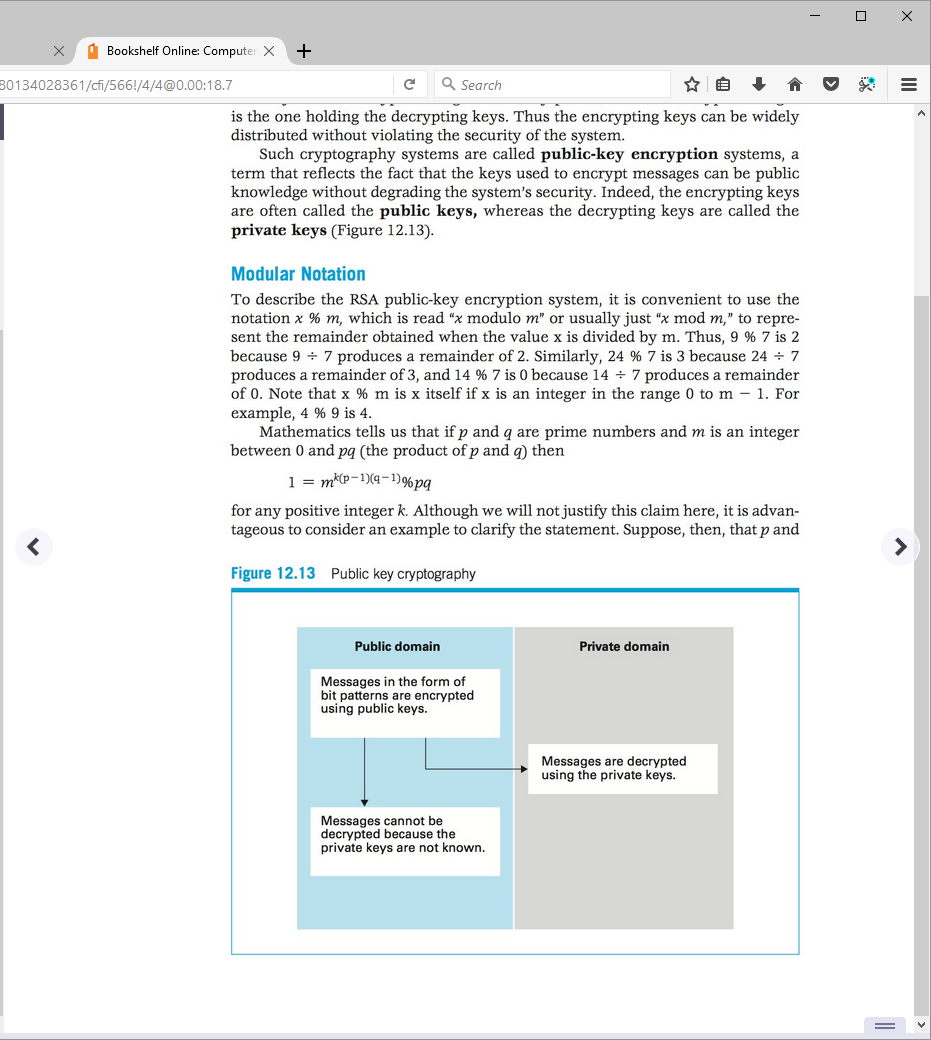
**CHAPTER 0-6**

**cryptography**

* In some cases the fact that a problem is difficult to solve has been turned into an asset rather than a liability.
* Of particular interest is the problem of finding the factors of a given integer—a problem for which an efficient solution has yet to be found, if one even exists.
* The failure to find an efficient way of determining the factors of large integers has long been a thorn in the side of many mathematicians, but in the field of cryptography it has been applied to produce a popular method of encrypting and decrypting messages known as the RSA algorithm.
* The RSA algorithm encrypts messages using one set of values known as the encrypting keys and decrypting those messages using another set of values known as the decrypting keys.
  + People who know the encrypting keys can encrypt messages, but they cannot decrypt messages.
  + The only person who can decrypt messages is the one holding the decrypting keys.
  + Thus the encrypting keys can be widely distributed without violating the security of the system.
* Cryptography systems such as the RSA algorithm are called public-key encryption systems, a term that reflects the fact that the keys used to encrypt messages can be public knowledge without degrading the system’s security.
  + Indeed, the encrypting keys are often called the public keys, whereas the decrypting keys are called the private keys.



**RSA Public-Key Cryptography**

* First we pick 2 distinct prime numbers p and q, and let pq=n.
* Then we pick 2 other positive integers e and d such that ed = k(p-1)(q-1)+1,for some positive integer k.
  + First we pick e, which must be:
    - An integer
    - Cannot be p or q
    - Relatively prime to (p-1)(q-1).
    - 1<e<(p-1)(q-1)
  + Then we pick d, which must be:
    - An integer
    - Satisfy ed = k(p-1)(q-1)+1,for some positive integer k
* Note that we have selected 5 values: p, q, n, e, and d.
  + The values e and n are the encrypting keys.
  + The values d and n are decrypting keys.
  + The values p and q are only used for constructing the encryption system.
* To encrypt a message (encoded as a bit string, perhaps using ASCII or Unicode):
  + Let the value of the bit string be m.
  + We will make sure m<n (if it is not, we would chop the message into smaller segments and encrypt each segment individually).
  + Then, the encrypted message is the binary representation of the value me % n.
* To decrypt a message (encoded as a bit string):
  + Let the value of the bit string be c.
  + Compute cd % n. This remainder will be the value m of the original message.

//Example0-1

Suppose we pick p= 7 and q=13, and n=7\*13=91. Find e and d.

//Example0-2

Encrypt the binary bit string 10111 using the encrypting keys n = 91 and e = 5. Give your answer in the form of a binary bit string.

//Example0-3

Decrypt the binary bit string 100 using the decrypting keys n = 91 and d = 29. Give your answer in the form of a binary bit string.

* n summary, an RSA public-key encryption system is generated by selecting two prime integers, p and q, from which the values n, e, and d are generated.
* The security of this system is based on the assumption that knowing the encrypting keys n and e does not allow one to compute the decrypting key d (n is known).
  + However, there are algorithms for doing exactly that!
* If we know the public keys n and e, we can find the private key d using the following algorithm:
  + Factor n to discover the prime numbers p and q such that pq=n.
  + Find a value k such that k(p-1)(q-1)+1 is evenly divided by e. The quotient would be d.
* However, the first step in this process can be time-consuming—especially if the values of p and q were chosen to be large.
  + In fact, if p and q are so large that they require hundreds of digits, then the best known factoring algorithms would require years before the identities of p and q could be revealed from n.
  + The strength of RSA is measured in the number of bits in n.
    - 512-bit (155 digit) RSA is no longer considered secure, as modern brute force attacks can extract private keys in just hours.
    - As of 2016, 1024-bit (309 digit) RSA is considered risky.
    - Nowadays, 4096-bit (1234 digit) RSA is commonly used.
* To this date, no one has found an efficient way of decrypting messages based on RSA cryptography without knowing the decrypting keys, and thus public-key encryption based on the RSA algorithm is widely used to obtain privacy when communicating over the Internet.

**HW**

1. Find the factors of 66,043.

66043=1\*\_\_\_\_\*\_\_\_\_\*\_\_\_\_\*…

1. Using the public keys n = 91 and e = 5, encrypt the binary bit string 101. Give your answer in the form of a binary bit string.
2. Using the private keys n = 91 and d = 29, decrypt the binary bit string 10. Give your answer in the form of a binary bit string.
3. Find the appropriate value for the decrypting keys n and d in an RSA public-key cryptography system based on the primes p = 7 and q = 19 and the encryption key e = 5.
4. Write a program to read in an integer (long) and display all pairs of factors of the input integer. That is, the output must be given as a list of pairs of factors such that the product of each pair is the input integer. Then, print which of these pairs contains only prime numbers (there can be either 1 such pair or none). Note that
   1. the Scanner class supports a nextLong method to read a long integer, nextBigInteger to read a BigInteger, and nextBigDecimal to read a BigDecimal.
   2. the printf method uses %d for int, long, BigInteger; and %f for float, double, and BigDecimal.

