

## LAB 2

### Key Recovery and Key Escrow

One of the problems with any type of encryption system – public-key or secret-key – is *key management*. Decryption keys and moduli are usually very long numbers that are impossible for most human beings to remember. Face it: many people have trouble remembering their passwords or PINs, much less a 100- or 200-digit key. The solution is to store these numbers on a secondary memory device that's not easily accessible by unauthorized "third parties"<sup>1</sup> (perhaps on a diskette that one keeps in a secure place). There are two possible problems:

- Even a key that is kept in a secure location can be *compromised* – discovered or stolen by an unauthorized third party. Anyone who suspects that his/her key has been compromised should get a new key.
- The storage device on which the key is stored could be destroyed or corrupted. In either case, the key is lost. One possible solution is to ask a "trusted third party" maintain a copy of the key. This assumes that one can find such a trusted third party. An individual may be willing to trust a close friend, but this is not possible for a business.

A second solution is to split the key into two or more parts, and ask a *different* third party to store each part. The purpose of this laboratory exercise is to explore one method for doing this. This method is based on a famous mathematical theorem called the *Chinese Remainder Theorem*. To make things easy, you will be using three-digit keys.

This is also the basic idea behind the various "key-escrow" proposals from the United States government. All keys would be split into two or more parts, with each part entrusted to a different public or private agency. The idea is that the police could recover the key without the individual's knowledge by obtaining warrants against each of the escrowing agencies. This would permit the police to "listen in" on encrypted communications or to read encrypted files without the key holder's knowledge. We will be discussing these proposals in class.

---

<sup>1</sup> The sender and receiver of the encrypted message – usually called Alice and Bob – are the first and second party.

1. Launch Excel and open the file

### **keyshare.xls**

Choose **Add-Ins** from the **Tools** menu, and be sure that the **Analysis ToolPak** is checked.

2. Click on the tab for labeled **Key Splitting**. This reveals a worksheet for splitting a three-digit key into three parts.
3. Select a three-digit key value. Enter this value in cell B6. Record this value below:

\_\_\_\_\_

4. If they're not already there, enter the values 11, 13 and 16 in cells B14, B15 and B16, respectively. These values are your *moduli*.<sup>2</sup> (It is not absolutely necessary to use the three moduli above. You could choose any three numbers between the cube root of 1000 – 10 – and the square root of 1000 – approximately 31 – such that no pair of moduli has any common factor larger than 1. For example, you could choose 14, 15 and 23.)

Record your three moduli below:

\_\_\_\_\_

5. The spreadsheet will split your key into three pieces by dividing by each of the moduli and taking the remainder. The three pieces of your key will appear in cells C14, C15 and C16. Record the values of these pieces below:

\_\_\_\_\_

6. In reality, one would ask three different parties to each store one piece. Instead, write down your three moduli and the corresponding three pieces on sheet of paper and exchange pieces with a student at another computer.
7. Click on the tab labeled **Key Recovery**. This reveals a worksheet for recovering a key from its three parts.

---

<sup>2</sup> Moduli is the plural of *modulus*, a term you encountered in the first encryption exercise. These moduli are not really the same as the modulus in the RSA public-key encryption method. However, they are both applications of the same basic mathematical concept.

8. Enter the *other student's* moduli in cells B7, B8 and B9. Enter her/his corresponding key pieces in cells C7, C8 and C9. Record all six of these values below:

<u>Modulus</u>	<u>Corresponding piece</u>
_____	_____
_____	_____
_____	_____

The key recovery calculation takes place in cells C7:E9 and cell E11. It works as follows:

- In each row of column C, compute the products of the moduli in the other two rows. For example, if the moduli in column B are 11, 13 and 16, the corresponding cells in column C will contain  $13*16 = 208$ ,  $11*16 = 176$ , and  $11*13 = 143$ , respectively
- Each row in column D contains the *inverse* of the value in column C with respect to the modulus in column B. To see this, enter the following formula in cell F7:

**= MOD (C7\*D7,A7)**

**MOD** is a built-in function that divides its first argument by its second and takes the remainder. What value appears in cell when you enter this formula?

\_\_\_\_\_

Select the range F7:F9 and fill down. What values appear in cells F8 and F9?

F8: \_\_\_\_\_ F9: \_\_\_\_\_

All of these values should be 1. This illustrates the concept of an *inverse*.

- The “magic numbers” in column E are just the product of the inverse and the other moduli. Thus, the magic number in cell E7 is just  $C7*D7$ . Note that this is just the product of the number in cell C7 and its inverse.
- To recover the key, multiply each piece by the corresponding “magic number.” Divide the result by the product of the moduli and take the remainder. Because of the special way we have constructed the magic numbers, this calculation produces the original key.

The recovered key value should appear in cell E11. Record this value below. Check with the other student to see that you have correctly recovered her/his key.

Prepare a short report of the lab.