Whatcom COMMUNITY COLLEGE

NCyTE CENTER

SYMMETRIC AND PUBLIC KEY ENCRYPTION LESSON

Mark Emry, McNeil High School, Round Rock ISD, Austin, TX

This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

Additional materials may be found at www.ncyte.net

SYMMETRIC AND PUBLIC KEY ENCRYPTION

IN-CLASS UNPLUGGED PUBLIC KEY ENCRYPTION EXERCISE

At the beginning of class, the teacher should hand out the **Bob's Public Key Map** (Exhibit 1) and the **Bob's Private Key Map** (Exhibit 2). In this exercise, the two (2) Alices send an encrypted message to Bob consisting of a single number (preferably, less than 100). The Alices encrypt the message using **Bob's Public Key Map**. Once done, Bob decrypts the message from the Alices using **Bob's Private Key Map**. A **Bob's Public Key Map** and a representative **Bob's Private Key Map** have been included, Exhibits below.

The reason there are two (2) Alices is because there is a substantive (though not insurmountable) computational load to this exercise. The two (2) Alices will need to create the public encrypted message. This message will be visible to Eve. In order for this exercise to work successfully, the Alices should double check that the computations required to create **Bob's Public Key Map** are correct.

To start the exercise, Bob creates his **Bob's Private Key Map** from the blank **Bob's Public Key Map** (Exhibit 1). **Bob's Private Key Map** consists of 16 specifically connected dots. The dots are connected so that every dot in **Bob's Private Key** is connected to exactly three other dots. For purposes of this exercise, it is important that the students use exactly this dot configuration as the **Bob's Public Key Map** and as the basis for **Bob's Private Key Map**.

To create the **Bob's Private Key Map** from the **Bob's Public Key Map** (Exhibit 1), the students playing the role of Bob need to select four special dots so that all 16 dots in **Bob's Private Key Map** are connected to exactly one of these four selected dots. In this way, the four special dots interconnections are separate **and** inclusive of all 16 dots.

Students should make these four special dots larger than the others. It may take a few iterations to get this correct. The teacher should check to make sure that the four dots in **Bob's Private Key** Map are correctly selected. Once completed, these 16 dots with the four selected dots will constitute **Bob's Private Key Map**. Exhibit 2 illustrates a representative **Bob's Private Key Map** in which the four dot interconnections have been correctly identified.

To simplify this exercise, the teacher may choose for the students playing the role of Bob to use Exhibit 2 as **Bob's Private Key Map**. This will save those students one potentially confusing step.

The students playing the role of Bob should keep **Bob's Private Key Map** private and not share it with either of the two Alices or the snooping Eve.

In Step 1, the two Alices now need to do some work. First, they need to pick a *secret integer* (preferably, less than 50). This *secret integer* is their secret message, and they should not share it with Bob or the snooping Eve. Next, the two Alices need to fill in all 16 dots with a number so that the sum of the 16 numbers equals the *secret integer* which they want to pass to Bob. The student should write these 16 numbers in pencil because they are going to have to erase these 16 numbers as part of Step 2. The students playing the two Alices should keep this map secret from both Bob and the snooping Eve.

Now, for the hard bit: Step 2. The two Alices need to visit all 16 dots of the map which they have just created. For **each** of the 16 dots, the two Alices need to put another number. This second number is the **sum** of the three surrounding dots and the dot itself. The Alices should write this number in pen next to the number they penciled in as part of Step 1. When finished, **each** of the 16 dots will have a sum of four dots.

Once done, the last thing the two Alices need to do as part of Step 2 is to erase the original numbers which add up to the message which they want to send to Bob. If those numbers are left on **Bob's Public Key Map** a snooping Eve would be able to add those 16 numbers together thereby decrypting the message from the two Alices. Once Bob's Public Key Map contains only those sums created in Step 2, it will be impossible for Eve to decipher the original number.

At this point, the students playing the role of Alice should ask Eve to pass their message (in the form of **Bob's Public Key Map**) to Bob. Once Bob has his completed **Bob's Public Key Map** in hand, Bob then decrypts the fully completed **Bob's Public Key Map** by adding together the sums (received from the Alices) listed at the four enlarged secret dots as indicated **Bob's Private Key Map**.

Magically, the four enlarged secret dots in **Bob's Private Key Map** sum to the *secret integer* message which the two Alices wish to pass to Bob under the snooping eyes of Eve. Once done, Bob should reveal the integer message from the Alices.

 This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

EXHIBIT 1 BOB'S PUBLIC KEY MAY

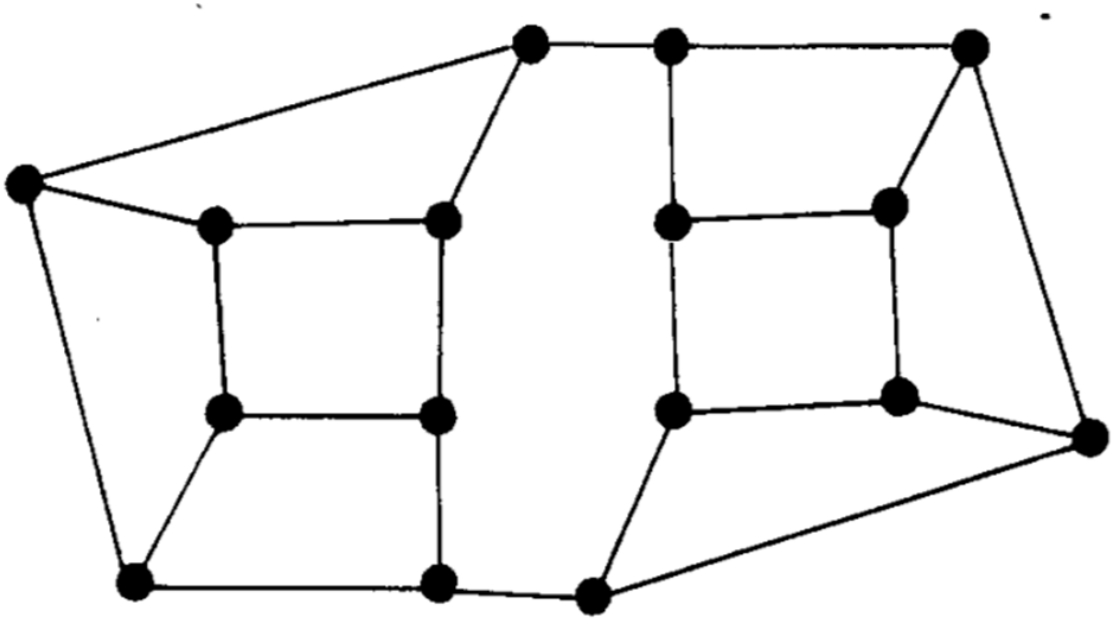

EXHIBIT 2 REPRESENTATIVE BOB'S PRIVATE KEY MAP