Kid Krypto—Public-key encryption

**Age group** - Junior high and up

**Time -** About 30 minutes.

**Size of group -** Requires at least two people, can be done with a whole class

**Focus -** Puzzle solving

Secret codes

**Summary -** Encryption is the key to information security. And the key to modern encryption is that using only public information, a sender can lock up their message in such a way that it can only be unlocked (privately, of course) by the intended recipient.

It is as though everyone buys a padlock, writes their name on it, and puts them all on the same table for others to use. They keep the key of course—the padlocks are the kind where you just click them shut. If I want to send you a secure message, I put it in a box, pick up your padlock, lock the box and send it to you. Even if it falls into the wrong hands, no-one else can unlock it. With this scheme there is no need for any prior communication to arrange secret codes.

This activity shows how this can be done digitally. And in the digital world, instead of picking up your padlock and using it, I copy it and use the copy, leaving the original lock on the table. If I were to make a copy of a physical padlock, I could only do so by taking it apart. In doing so I could inevitably see how it worked. But in the digital world we can arrange for people to copy locks without being able to discover the key!

Sounds impossible? Read on.

**Technical terms**

Public-key cryptosystems, encryption, decryption, NP-complete problems.

**Materials**

* + Divide the participants into groups of four, and within these groups form two subgroups.
	+ Each subgroup is given a copy of the two maps. (Handouts).
	+ An overhead projector transparency or other projection of maps, and a way to annotate the diagram.

**Procedure**

1. Project the public map for the entire class to see.
2. Pick a number to send.
3. To encrypt the number, place random numbers on each intersection on the map, so that the random numbers add up to the number that you are sending. (Example below)



1. The figure shows an example of such numbers as the upper (non-parenthesised) number beside each intersection. Here, the number being sent is 66, so all the unbracketed numbers add up to 66. If necessary, you can use negative numbers to get the total down to the desired value.
2. Now we must calculate what to send. If we sent the map with the numbers on, that would be no good, because if it fell into the wrong hands anybody could add them up and get the message.
3. Choose any intersection. Look at it and its three neighbors—four intersections in all—and total the numbers on them. Write this number at the intersection in parentheses or using a different color of pen. For example, the rightmost intersection in the figure is connected to three others, labeled 1, 4, 11, and is itself labeled 6. Thus it has a total of 22. Now repeat this for all the other intersections in the map. This should give you the number in parentheses in the figure.
4. The map will be sent with only the parenthesized numbers on it.
5. Erase the original numbers and the counts, leaving only the numbers in parentheses, or write out a new map with just those numbers on it. See if any of the students can find a way to tell from this what the original message was. They won’t be able to.
6. To decode the message you need the private map with its private key.
7. On the coded message mark the special enlarged nodes on the private map (Figure below).



**Private Map**

1. To decode the message, look at just the secret marked intersections and add up the numbers on them. In the example, these intersections are labeled 13, 13, 22, 18, which add up to 66, the original message.
2. How does it work? Choose one of the marked intersections and draw around the intersections one street distant from it, and repeat the procedure for each marked intersection. This will partition the map into non-overlapping pieces, as illustrated in the figure below. 
3. The group of intersections in each partition is exactly the ones summed to give the transmitted numbers for the marked intersections, so the sum of the four transmitted numbers on those intersections will be the sum of all the original numbers in the original map; that is, it will be the original message
4. Having been through one example with the whole class, divide the students into groups four.
5. Give each pair of each group the public map.
6. Each pair should choose a “message” (any integer), encode it with the public key, and give the resulting map to the other group.
7. The other group can try to decode it, but they are unlikely to be successful until they are given (or work out!) the private map.
8. Then give out the private map and see if they can now decode it correctly

Phew! It seems a lot of work to send one letter. And it is a lot of work to send one letter—

encryption is not an easy thing to do. But look at what has been accomplished: complete secrecy using a public key, with no need for any prior arrangement between the participants. You could publish your key on a noticeboard and anyone could send you a secret message, yet no-one could decrypt it without the private key. And in real life all the calculation will be done by a software package that you acquire, so it’s only a computer that has to work hard.