6 Grade 6: RSA Cipher

6.1 The Activity

This is a game with two players or teams. The players take turns selecting either prime or composite numbers as outlined on the board below. The key is that the product of the numbers chosen have to be equal. Here is a sample game:

After Move 1

Team A			=	Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
8	×		=		×	
Composite Number		Prime Number		Prime Number		Composite Number

After Move 2

Team A			=	Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
8	×		=	2	×	
Composite Number		Prime Number		Prime Number		Composite Number

After Move 3

Team A			=	Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
8	×	7	=	2	×	
Composite Number		Prime Number		Prime Number		Composite Number

Team B can now win the game if he can find a composite number to make the equation true. If Team B can not make the equation equal, then Team A wins.

After Move 4

Team A			=	Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
8	×	7	=	2	×	28
Composite Number		Prime Number		Prime Number		Composite Number

Keep the initial composite number 12 or less for the initial games. Then, move this to 50 or higher if you like.

Here are some questions:

- Which team is most likely to win? Is there a winning strategy?
- "Can I use a calculator?"

6.2 RSA Gameboards

Team A				Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
	×		=		×	
Composite Number		Prime Number		Prime Number		Composite Number

Team A				Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
	×		=		×	
Composite Number		Prime Number		Prime Number		Composite Number

Team A				Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
	×		=		×	
Composite Number		Prime Number		Prime Number		Composite Number

Team A				Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
	×		=		×	
Composite Number		Prime Number		Prime Number		Composite Number

Team A				Team B		
Move 1	×	Move 3	=	Move 2	×	Move 4
	×		=		×	
Composite Number		Prime Number		Prime Number		Composite Number

6.3 The Mathematical Problem

Break the RSA code, proposed by Rivest, Shamir and Aldeman in 1978:

Find a reliable way for Team B to win.

6.4 More Details and More Ideas

Here is an example of how RSA really works (taken from [5]). We start with assuming Team B wants to send Team A a message (and that message is a number).

1. Team A selects two prime numbers. We will use $p = 23$ and $q = 41$ for this example, but keep in mind that the real numbers person A should use should be much much larger.

2. Team A multiplies p and q together to get $pq = (23)(41) = 943$. 943 is the "public key", which he tells to person B (and to the rest of the world, if he wishes).

3. Team A also chooses another number e which must be relatively prime to $(p-1)(q-1)$. In this case, $(p-1)(q-1) = (22)(40) = 880$, so $e = 7$ is fine. e is also part of the public key, so B also is told the value of e.

4. Now B knows enough to encode a message to A. Suppose, for this example, that the message is the number $M = 35$.

5. B calculates the value of $C = M^e \pmod N = 35^7 \pmod{943}$.

6. $35^7 = 64339296875$ and $64339296875 \pmod{943} = 545$. The number 545 is the encoding that B sends to A.

7. Now A wants to decode 545. To do so, he needs to find a number d such that $ed = 1 \pmod{(p-1)(q-1)}$, or in this case, such that $7d = 1 \pmod{880}$. A solution is $d = 503$, since $7 \cdot 503 = 3521 = 4 \cdot 880 + 1 = 1 \pmod{880}$.

8. To find the decoding, A must calculate $C^d \pmod N = 545^{503} \pmod{943}$. This looks like it will be a horrible calculation, and at first it seems like it is, but notice that $503 = 256+128+64+32+16+4+2+1$ (this is just the binary expansion of 503). So this means that

$$545^{503} = 545^{256+128+64+32+16+4+2+1} = 545^{256}545^{128}545^{1}$$

But since we only care about the result $\pmod{943}$, we can calculate all the partial results in that modulus, and by repeated squaring of 545, we can get all the exponents that are powers of 2. For example, $545^2 \pmod{943} = 545 \cdot 545 = 297025 \pmod{943} = 923$. Then square again: $545^4 \pmod{943} = (545^2)^2 \pmod{943} = 923^2 = 851929 \pmod{943} = 400$, and so on. We obtain the

3.3 The Mathematical Problem

The *Graceful Tree Conjecture* was proposed by Ringel, Kitzig and Rosa in 1967:

> Start with a tree and label the vertices with the consecutive odd numbers. Then, label the edges with the difference between the adjacent vertices. Can this always be done so that all edges are labeled differently?

3.4 More Details and More Ideas

1. If you do some research, the graceful tree conjecture sounds a little different from what we have stated. Instead, you label the m vertices with the numbers $0, 1, 2, \ldots, m-1$ and label the edges with these differences and you want the edge labelings to be unique. Why is this the same as the definition we used?

2. The number of possible trees with a given number of vertices can be quite high. For example, there are nearly 110 billion trees with 32 vertices. Thus, if you wanted to test all these trees to see if they are graceful, then you would have to test an enormous number of trees. This has, in fact, been done for trees with 35 or less vertices: all trees with 35 or less vertices are graceful.

3. You could clearly investigate this with more and more vertices. But, it might also be interesting to allow non-connected trees (so you can't get from one vertex to every other vertex). Or, you could try it with graphs (so that there are loops).