RSA AND THE MIRACLE OF PUBLIC-KEY ENCRYPTION

MATH CIRCLE (BEGINNERS) 03/18/2012

Recall for two numbers x and y:

x and y are ____________________ $\iff$ $\gcd(x, y) =$ _____

$\iff$ x and y have no ____________________in common

$\iff$ __________ $= \phi(x) \cdot \phi(y)$

$\iff$ there exist integers a and b with $ax + by = 1$.

(And remember Euler's phi function $\phi(n)$ is defined as the number of numbers between 1 and n, which are relatively prime to _________.)

For modulus 11 below, fill in the table with the powers of your choice of three different numbers relatively prime to 11 (you can't pick 1, that's too easy), and see how long it takes each of the powers to cycle. An example column is done for you with 9 (so you can't pick 9, either!).

Modulus 11

# rel. prime to 11:	9			
to power 1	$9^1 \equiv 9 \pmod{11}$			
to power 2	$9^2 \equiv 4 \pmod{11}$			
to power 3	$9^3 \equiv 3 \pmod{11}$			
to power 4	$9^4 \equiv 5 \pmod{11}$			
to power 5	$9^5 \equiv 1 \pmod{11}$			
to power 6	$9^6 \equiv 9 \pmod{11}$			
to power 7	$9^7 \equiv 4 \pmod{11}$			
to power 8	$9^8 \equiv 3 \pmod{11}$			
to power 9	$9^9 \equiv 5 \pmod{11}$			
to power 10	$9^{10} \equiv 1 \pmod{11}$			
to power 11	$9^{11} \equiv 1 \pmod{11}$			
pattern	9,4,3,5,1			
length of pattern	5			

No matter what three numbers you chose to fill in the chart with, you should have seen that in each column, the number 1 appears as the 10th number in the cycle. (And it *first* appears as either the 1st, 2nd, 5th, or 10th number in the cycle... all the factors of 10.) This is no coincidence, and it has to do with the fact that $\phi(11) = 10$. The following Theorem shows us this will always happen for relatively prime modulus and number which we raise to powers:

Euler's Theorem: If a and m are relatively prime, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

We can use this to more easily calculate some powers $\pmod{m}$. For example, to compute $7^{182} \pmod{37}$ (note 7 and 37 are relatively prime). Since $\phi(37) = 36$, we know directly by Euler's Theorem that $7^{36} \equiv 1 \pmod{37}$.

Divide the actual exponent we're interested in–182–by 36. We get $182 = 5 \cdot 36 + 2$. Therefore:

$7^{182} = 7^{5 \cdot 36 + 2} = 7^{36 \cdot 5 + 1} = (7^{36})^5 \cdot 7^2 \equiv 1^5 \cdot 7^2 = 7^2 = 49 \equiv 12 \pmod{37}$.

Now try some of your own:

(1) $5^{72} \pmod{36} =$

(2) $10^{2012} \pmod{31} =$

(3) $2^{187} \pmod{77} =$

(4) $823^{801} \pmod{1000} =$

(5) $11^{83} \pmod{43} =$

(Hint: This one's trickier than the previous ones...)

Setup:

Bob wants everybody to send him secret messages! So he sets up an RSA public key. Here are the steps he takes:

(S1) First Bob chooses two big, random prime numbers, p and q, and multiplies them together to get $N = p \cdot q$.

(S2) Next Bob multiplies $p-1$ and $q-1$ to get $\phi(n) = (p-1) \cdot (q-1)$. He chooses a random number d, ($1 \leq d \leq \phi(N)$) that's relatively prime to $\phi(N)$ and N.

(S3) Bob uses the Extended Euclidean Algorithm to compute the inverse of $d \pmod{\phi(N)}$, that is: a number e such that $d \cdot e \equiv 1 \pmod{\phi(N)}$.

(S4) Finally, Bob publishes the values e and N in the phone book so everyone can see–they are Bob's public key. He keeps d (and N) written down somewhere private; d is the secret key.

Encryption

Now when Alice wants to send a secret message m to Bob, she does just one step: (m must be relatively prime to N)

(E1) Alice looks up Bob's name in the phone book and find his public key (e, N). She computes the ciphertext $c = m^e \pmod{N}$, and sends it to Bob. (*Notice she doesn't need to know Bob's secret key d–she never uses it!)*

Decryption

Bob gets Alice's ciphertext c, and wants to decrypt it.

(D1) Bob computes $m = (c^d \equiv \pmod{N})$.

Do your own example with specific (small) numbers! Recommendation: Choose $p = 7$, $q = 11$, $d = 13$, and $m = 17$.

Setup:

(S1) First Bob chooses two big, random prime numbers, p and q, and multiplies them together to get $N = p \cdot q$.

$p =$

$q =$

$N =$

(S2) Next Bob multiplies $p-1$ and $q-1$ to get $\phi(N) = (p-1) \cdot (q-1)$. He chooses a random number d ($1 \leq d \leq \phi(N)$) that's relatively prime to $\phi(N)$ and N.

$\phi(N) =$

$d =$

(S3) Bob uses the Extended Euclidean Algorithm to compute the inverse of $d \pmod{\phi(N)}$, that is: a number e such that $d \cdot e \equiv 1 \pmod{\phi(N)}$.

$e =$

(S4) Bob publishes e and N and writes down d as the secret key.

Encryption

Alice's message (must be relatively prime to N): $m =$

(E1) Alice looks in the phone book and find Bob's public key (e, N). She computes the ciphertext $c = m^e \pmod{N}$, and send it to Bob.

$c =$

Decryption

(D1) Bob computes $m = (c^d \pmod{N})$.

$m =$

(You already know m–but go ahead and compute $c^d \pmod{N}$ anyway, just to check!)