Public Key Cryptosystems - RSA

$p$ and $q$ prime

$57$ 
$q$ 
$41$ 

$53$ 
$q$ 
$47$ 

$17$ 
$p$ 
$19$ 
$q$
Public Key Cryptosystems - RSA

Compute numbers $n = p \times q$

$p$ and $q$ prime

$p = 53$
$q = 47$

$n = 2337$

$2337 = p \times q$

$323$ is a factor of $n$

$2491$ is another factor of $n$
Public Key Cryptosystems - RSA

Choose $e$ prime relative to $(p-1)(q-1)$

$p$ and $q$ prime

$57$ $p$
$q$ $41$

$43$

$2337$

$323$ $23$
$p$
$q$

$41$

$2491$

$53$
$q$

$47$

$17$
$p$
$q$
Public Key Cryptosystems - RSA

Publish \(<n,e>\) pair as the public key

\[ p = 57 \quad q = 41 \]

\[ n = 2337 \quad e = 43 \]

\[ p = 53 \quad q = 47 \]

\[ n = 2337 \quad e = 43 \]

\[ p = 53 \quad q = 47 \]

\[ n = 2337 \quad e = 43 \]

\[ n = 2491 \quad e = 41 \]

\( p \) and \( q \) prime
Public Key Cryptosystems - RSA

Find $d$ such that $(e \cdot d - 1)$ is divisible by $(p-1)(q-1)$

$p$ and $q$ prime
Public Key Cryptosystems - RSA

Keep $<d, n>$ as the private key

$p$ and $q$ prime
Public Key Cryptosystems - RSA

Toss $p$ and $q$

Sender

Receiver

Attacker

1667
2337
43

263
323
23

2217
2491
41
Public Key Cryptosystems - RSA

Receiver

Sender

Attacker

\[ m^{43} \mod 2337 \]
Public Key Cryptosystems - RSA

$(m^{43} \mod 2337)^{1667} \mod 2337$
Public Key Cryptosystems - RSA, signing

\[ m^{263} \mod 323 \]
Public Key Cryptosystems - RSA, signing

$\left( m^{263} \mod 323 \right)^{23} \mod 323$
Public Key Cryptosystems - RSA, exponentiating

\[ 25663^{55637} \mod 78837 \]
Public Key Cryptosystems - RSA, exponentiating

\[ 25663^{55637} \mod 78837 \] Yikes!
Public Key Cryptosystems - RSA, exponentiating

\[ 25663^{55637} \mod 78837 \quad \text{Yikes!} \]

Rescued by:

\[ a^x b^y \mod p = (a^x \mod p)(b^y \mod p) \mod p \]
Public Key Cryptosystems - RSA, exponentiating

\[ 25663^{55637} \mod 78837 \]

\[ 25663^2 \mod 78837 \]

... 

That is, do the modular reduction after each multiplication.
Public Key Cryptosystems - RSA, find primes

Probability that a random number $n$ is prime: $\frac{1}{\ln(n)}$

For 100 digit number this is $1/230$. 
Public Key Cryptosystems - RSA, find primes

Probability that a random number $n$ is prime: $1/\ln(n)$
For 100 digit number this is $1/230$.
But how to test for being prime?
Public Key Cryptosystems - RSA, find primes

Probability that a random number $n$ is prime: $1/\ln(n)$

For 100 digit number this is $1/230$.

But how to test for being prime?

If $p$ is prime and $0 < a < p$, then $a^{p-1} = 1 \mod p$

Ex: $3^{(5-1)} = 81 = 1 \mod 5$
$36^{(29-1)} = 37711171281396032013366321198900157303750656$
$= 1 \mod 29$
Probability that a random number $n$ is prime: $1/\ln(n)$

For 100 digit number this is $1/230$.

But how to test for being prime?

If $p$ is prime and $0 < a < p$, then $a^{p-1} = 1 \mod p$

*Ex:* $3^{(5-1)} = 81 = 1 \mod 5$

$36^{(29-1)} = 37711171281396032013366321198900157303750656$

$= 1 \mod 29$

$Pr (p \text{ isn't prime but } a^{p-1} = 1 \mod p) \rightarrow \text{very tiny number}$

(See http://gauss.ececs.uc.edu/Courses/c653/lectures/Math/Fermat/fermat.html)
Public Key Cryptosystems - RSA, find primes

But we need some help to use the above -

Define: trivial square roots of 1 mod $p$: $1 \mod p$ and $-1 \mod p$

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>...</th>
<th>$p-2$</th>
<th>$p-1$</th>
</tr>
</thead>
</table>

1 mod $p$                      -1 mod $p$

Fact 1: If $p$ is prime, there are no non-trivial square roots of 1 mod $p$

Let $x > 1$ be a square root of 1 mod $p$. Then $x^2 = 1 \mod p$.
Or, $(x-1)(x+1) = 0 \mod p$, so that $p$ divides $(x-1)$ or $(x+1)$.
But a prime can divide $(x-1)$ only if $x = 1 \mod p$
and can divide $(x+1)$ only if $x = -1 \mod p$

Note: if $p=16$, $x=7$ then $(x+1) = 0 \mod p$ and $x^2 = 1 \mod p$
so, in this non-prime case, $x$ other than -1 or +1 is a square root
Fact 2: If $p$ is prime, the exponent $p-1$ is an even number
Fact 2: If $p$ is prime, the exponent $p-1$ is an even number.

Fact 3: If $p$ is not prime then the probability that there is a square root of $a^{p-1} \mod p$ that is neither $1 \mod p$ nor $-1 \mod p$ is not greater than $1/4$, assuming $a$ is an integer chosen randomly between 1 and $p-1$. 
Public Key Cryptosystems - RSA, find primes

**Fact 2:** If $p$ is prime, the exponent $p-1$ is an even number.

**Fact 3:** If $p$ is not prime then the probability that there is a square root of $a^{p-1} \mod p$ that is neither $1 \mod p$ nor $-1 \mod p$ is not greater than $1/4$, assuming $a$ is an integer chosen randomly between 1 and $p-1$.

**An algorithm to test $p$ for being a prime number:**

If $p$ is even, return \textit{false} ($p$ is not prime)

Repeat the following at most 100 times:

Choose a random integer $a$ such that $0 \leq a < p$.

If some square root of $a^{p-1} \mod p$ is neither $1 \mod p$ nor $-1 \mod p$ then return \textit{false} ($p$ is not prime).

Return \textit{probably} ($p$ is prime with $2^{-200}$ probability of error)
Public Key Cryptosystems - RSA, find primes

Can always express integer $p-1$ as $2^b m$ for some odd number $m$

Ex: $428 = 2^2 \times 107$

Here is the $2^b$ ($b = 2$)

\[110101100\]

Here is the odd number ($m = 107$)

Instead of finding the square root of $a^{p-1} \mod p$, write $p-1 = 2^b m$ then check whether $a^m \equiv 1 \mod p$. If so, there are no non-trivial square roots. Otherwise check whether $a^{m^2} \equiv 1 \mod p$. If so and if the square root of the left side is $a^m \mod p$ which, if not equal to -1 mod $p$, must be a non-trivial root of unity of $a^{m^2} \mod p$ and therefore $a^{m^2} \mod p$. If $a^{m^2} \not\equiv 1 \mod p$ then repeat for $a^{m^2^2}$ and so on, possibly up to $a^{m^2^b}$.

(See http://gauss.ececs.uc.edu/Courses/c653/lectures/Math/PrimesTest/mr.html)
Choose $e$ first, then find $p$ and $q$ so $(p-1)$ and $(q-1)$ are relatively prime to $e$.

RSA is no less secure if $e$ is always the same and small.

Popular values for $e$ are 3 and 65537.

For $e = 3$, though, must pad message or else ciphertext = plaintext.

Choose $p \equiv 2 \mod 3$ so $p-1 = 1 \mod 3$.

So, choose random odd number, multiply by 3 and add 2, then test for primality.