Lecture 8 RSA

RSA uses the difficulty of solving exponential congruences such as we are discussed in the following propositions.

Proposition: Let p be a prime and $e \ge 1$ an integer for which $\gcd(e, p-1) = 1$. Let d be the inverse of e mod $p - 1$ (so $de \equiv 1 \pmod{p-1}$). Then the congruence $x^e \equiv c \pmod{p}$ has the unique solution $x \equiv c^d \pmod{p}$.

Pf: Consider the following two cases.
Case 1: $c \equiv 0 \pmod{p}$ which implies that $x \equiv 0 \pmod{p}$ is the unique solution.

Case 2: $c \not\equiv 0 \pmod{p}$ We have $de \equiv 1 \pmod{p-1} \Rightarrow de = 1 + k(p-1)$ for some integer k. Then $(c^d)^e \equiv c^{de} \equiv c^{1+k(p-1)} \equiv c*(c^{p-1})^k \equiv c*1 \equiv c \pmod{p}$ (where we used Fermat's Little Theorem).

Therefore $x \equiv c^d \pmod{p}$ is a solution of $x^e \equiv c \pmod{p}$. Next we prove that this solution is unique.

Suppose x_1, x_2 are both solutions to $x^e \equiv c \pmod{p}$. Then we have
$x_1 \equiv x_1^{de} \equiv (x_1^e)^d \equiv c^d \equiv (x_2^e)^d \equiv x_2^{de} \equiv x_2 \pmod{p}$.

Ex. (1) Solve $x^{11} \equiv 14 \pmod{17}$. First we find 11^{-1} mod 16, $11^{-1} \equiv 3 \pmod{16}$.
Then $x \equiv 14^3 \equiv 7 \pmod{17}$ is our solution.

(2) Solve $x^{1583} \equiv 4714 \pmod{7919}$ (7919 is prime). First we find
1583^{-1} mod 7918, $1583^{-1} \equiv 5277 \pmod{7918}$. Then $x \equiv 4714^{5277} \equiv 6059 \pmod{7919}$ is our solution.

We now look at three generalizations of this proposition.

Proposition A Let $n = pq$, where p,q are distinct primes, and $e \ge 1$ an integer for which $\gcd(e, p-1) = 1$. Let $d \equiv e^{-1} \pmod{(p-1)(q-1)}$ (so $de \equiv 1 \pmod{(p-1)(q-1)}$). Then the congruence $x^e \equiv c \pmod{n}$ has the unique solution $x \equiv c^d \pmod{n}$.

Proposition B Let $n = pq$, where p,q are distinct primes, and $e \ge 1$ an integer for which $\gcd(e, p-1) = 1$. Let $g = \gcd(p-1, q-1)$ and $d \equiv e^{-1} \pmod{(p-1)(q-1)/g}$. Then the congruence $x^e \equiv c \pmod{n}$ has the unique solution $x \equiv c^d \pmod{n}$.

Proposition C Given a positive integer n. Let c be an integer for which $\gcd(c,n) = 1$ and $e \ge 1$ an integer for which $\gcd(e, \phi(n)) = 1$. Let $d \equiv e^{-1} \pmod{\phi(n)}$. Then the congruence $x^e \equiv c \pmod{n}$ has the unique solution $x \equiv c^d \pmod{n}$.

Pf. We will prove C. Since $de \equiv 1 \pmod{n}$ we may write $de = 1 + k\phi(n)$ for some integer *k*. Let $x \equiv c^d \pmod{n}$. Then $x^e \equiv (c^d)^e \equiv c^{de} \equiv c^{1+k\phi(n)} \equiv c(c^{\phi(n)})^k \equiv c(1)^k \equiv c \pmod{n}$

We need to show that this *x* is the unique solution. Suppose there were two values x_1, x_2 both satisfy $x^e \equiv c \pmod{n}$. Then $x_1 \equiv x_1^{de} \equiv (x_1^e)^d \equiv c^d \equiv (x_2^e)^d \equiv x_2^{de} \equiv x_2 \pmod{n}$. So these solutions are equal mod *n*.

RSA Algorithm

RSA (Rivest – Shamir – Adleman) was first published in 1978.

Bob chooses a large integer *N* which is a product of two primes $N = pq$ .Bob also chooses a positive integer *e* such that $\gcd(e, (p-1)(q-1)) = 1$. Bob then publishes the public key (N, e).

Alice then uses this key to encode a message *m*, by computing $c \equiv m^e \pmod{N}$. Alice then sends the coded message c to Bob.

Bob decodes the message by first computing the inverse *d* of *e*, $d \equiv e^{-1} \pmod{(p-1)(q-1)}$. Note this inverse is mod (*p*-1)(*q*-1) **not** mod ***n***. Bob then retrieves the original message by $m \equiv c^d \pmod{N}$.

Why does this work? An intruder Eve can find out the values of N, e, c . To decode the message Eve would also need to find out the value of *d*. But this would require computing $e^{-1} \mod (p-1)(q-1)$. This would require factoring ***N***. But ***N*** is a large number (and both prime factors are large).In general factoring large numbers is not easy to do.

Examples
(1) Let $p = 5, q = 7, N = 5*7 = 35$. We need to choose e so that e is relatively prime to $(p-1)(q-1) = 24$. Let's use $e = 17$. Bob sends the public key (35, 17) to Alice.

Alice uses the message $m = 25$. This encodes to $c \equiv m^e \equiv 25^{17} \equiv 30 \pmod{35}$. Alice then sends the code 30 to Bob.

Bob first computes $d \equiv e^{-1} \equiv 17^{-1} \equiv 17 \pmod{24}$. Bob then decodes the message by $c^d \equiv 30^{17} \equiv 25 \pmod{35}$, which is the correct original message.

(2) Let $p = 3019, q = 4363, N = pq = 13171897$. We need to choose e so that e is relatively prime to $(p-1)(q-1) = 13164516$. Let's use $e = 2191067$. Bob sends the public key (13171897, 2191067) to Alice.

Alice uses the message $m = 5767534$. This encodes to $c \equiv m^e \equiv 6715666 \pmod{N}$. Alice then sends this code to Bob.

Bob first computes $d \equiv e^{-1} \equiv 2589443 \pmod{4382136}$. Bob then decodes the message by $c^d \equiv 5767534 \pmod{N}$, which is the correct original message.

Attacks on RSA

Modulus Attack

Theorem:
(1) If the private key *d* is known then $n = pq$ can be factored.
(2) If the factors $n = pq$ are known then the private key *d* can be computed.

Pf: (1) Suppose *d* is known. We already know the public key *e* where $d \equiv e^{-1} \pmod{\phi(n)}$. Then we have $de = 1 + k\phi(n)$ for some integer *k*. Let $t = k\phi(n)$, then *t* is even (since $\phi(n) = (p-1)(q-1)$ is an even number) and $de - 1 = t$.

By Euler's Theorem, for every $g \in \mathbb{Z}_N^*$, $g^{\phi(n)} \equiv 1 \pmod{n} \Rightarrow g^t \equiv 1 \pmod{n}$. Using the Chinese Remainder Theorem one can show that this has four possible solutions: $\pm 1, \pm x$ where x satisfies $x \equiv 1 \pmod{p},\ x \equiv -1 \pmod{q}$. In this case $\gcd(x-1, n) = p$. So knowing x we can find p and then find q.

(2) Suppose that the factors p,q are known. Then $\phi(n) = (p-1)(q-1)$ is known and $d = e^{-1} \pmod{\phi(n)}$ can be computed.

Common modulus

Suppose that every in an encryption system uses the same modulus $n = pq$. But everyone uses their own encryption/ decryption keys (e,d).

By the above theorem, Bob can then use his keys (e_B, d_B) to factor *n*. Once he has the factors p,q he can then find Alice's decryption key d_B (again using the above theorem). Bob is also able to compute Alice's encryption key $e_B = d_B^{-1}$.

The moral is that the RSA modulus should never be used by multiple entities.

Small private exponent *d*

This is known as Wiener's attack. Let $n = pq$ and assume that $q < p < 2q$. Assume that the decryption key $d < \frac{1}{3} n^{1/4}$. Given a public key (n,e) with $ed \equiv 1 \pmod{\phi(n)}$.

With these assumptions d can be efficiently computed and n factored.

Outline of procedure. Suppose $de = 1 + k\phi(n)$ for some integer k, where $k < d$ and $\gcd(k,d) = 1$.

From the above assumptions one can show that

$$\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{1}{2d^2}$$

Since e, n are known, there are relatively few fractions $\frac{k}{d}$ which makes this inequality true. Once we find the fraction we find d and then we can factor n.

Small puble exponent e

This is known as Coppersmith's attack or method. If $f(x)$ is a polynomial with integer coefficients then the roots of $f(x)$ mod n are the values x_0 such that $f(x_0) \equiv 0 \pmod{n}$. If $|x_0| < n^{1/d}$ then these roots can be computed efficiently.

Def. A **pad** of bit length m is a sequence of r random bits used as follows. A message M is transformed to a message of the form $2^m M + r$ where $r \in \{0,1,\ldots,2^{m-1}\}$.

Theorem:
Let the public key (n,e) be known (with e small, for example $e = 3$). Suppose c_1, c_2 are two RSA encryptions of the same message M with pads r_1, r_2. One can then efficiently compute M.

Note the proof involves factoring polynomials $g_1(x) = x^e - c_1$, $g_2(x,y) = (x+y)^e - c_2$.