Notes on Encryption

Robert L. Walton

August 10, 1999

1 Information Source

The source of the information here is:

> Bruce Schneier, Applied Cryptography, John Wiley, 1996, ISBN 0-471-11709-9

2 Encryption by XORing with Random Bits

To encrypt a message, one may XOR it with a string of random or pseudo-random bits known to only the sender and receiver.

- If the string of random bits is truely random and is never reused, it is called a one-time pad. Such an encryption scheme is unbreakable.
- The string of random bits may be generated by a pseudo-random number generator using a key as a seed.

3 Pseudo-Random Number Generators

Example 1: Given a natural number $m < 2^{31} - 1$, generate a 'next number' equal to $7^5 \cdot m \pmod{2^{31} - 1}$. The sequence of numbers generated by this method (assuming the initial m is not zero) does not repeat until $2^{31} - 2$ numbers have been generated, and satisfies statistical tests for randomness fairly well.

Example 2: Consider numbers made from bit strings in which addition and subtraction have been changed so that they simply XOR bit strings, and multiplication and division use the algorithms of binary multiplication and division but with both addition and substraction replaced by XOR.

This gives a number system that is easier to compute with than standard numbers, because there are no carries.

Mathematically this number system is the same as polynomials in some variable x with coefficents in the integers modulo 2. Thus all the coefficents are either 0 or 1, and addition of coefficents is the same as XOR. Subtraction also turns out to be the same as XOR. Multiplication and division of such polynomials turns out to be like multiplication and division of binary numbers with addition and subtraction replaced by XOR.

In this number system there are primes, just as for the ordinary number system. If one picks a prime p, one can generate a sequence of numbers where the number after m is $2m \pmod p$. If the highest order 1 bit of p is the n'th bit, then m can be represented in $n-1$ bits (it must be a number mod p), and this algorithm can be implemented very efficiently in hardware: just shift the bits of m left to multiply by 2, and if a 1 was shifted out the high order end of m, XOR p into the result to subtract p and get an output that is '(mod p)'.

The resulting sequence of numbers does not repeat until $p-1$ numbers have been generated, and at least for many p, satisfies statistical tests for randomness fairly well. Pseudo-random numbers can be generated very fast by this method.

Example 3: If an adversary knows some of the text being encrypted, she can recover some of the random sequence being XORed with the text. If pseudo-random number generators like the above are being used, a small part of the pseudo-random sequence can give away the key (initial seed). This is because the pseudo-random algorithms are linear and easily analyzed by math.

To prevent this 'known plain text' attack (the 'plain text' is the text before encryption), real-world encryption schemes run several pseudo-random number generators at once and use the state of their outputs to determine which of the several generators to step next. Such systems of generators can be designed that are very hard to attack.

4 RSA

RSA (Rivest, Shamir, Adleman) is a public-key algorithm based on the difficulty of finding logrithms in modulo arithmetic, and on the difficulty of factoring a product of two very large prime numbers.

In a public key algorithm there are two keys, a public key and a private key. A message may be encrypted with either key, but must be decrypted with the other key. There is no way to deduce the private key even if you know the public key.

The idea of RSA is to find a very large number n and a pair of numbers e and d such that for every message $m < n$, $m^{ed} = m \pmod{n}$. Then $c = m^e \pmod{n}$ can be the encryption of m and $m = c^d \pmod{n}$ decrypts c.

n and e can be published as the public key, and d is the private key. It must be impossible to compute d from n and e.

RSA creates n by finding two very large prime numbers p and q, and setting $n = pq$. It follows from number theory that $m^{\phi(n)} = 1 \pmod{n}$ if m is relatively prime[1] to n, where $\phi(n) = (p-1)(q-1)$ is the Euler totient function. We will describe the relevant number theory below. We chose e to be relatively prime to $\phi(n)$ so that we can find d such that $ed = 1 \pmod{\phi(n)}$, where again the relevant number theory is below. Then for some integer k, $ed = k \cdot \phi(n) + 1$, and

$$m^{ed} = m^{k \cdot \phi(n)+1} = (m^{\phi(n)})^k \cdot m = 1^k \cdot m = 1 \cdot m \pmod{n}$$

for any m relatively prime to n.

Note that if m is not relatively prime to n this will not work. The totient function $\phi(n)$ is just the number of natural numbers less than n that are relatively prime to n. Since $n = pq$ and p and q are prime, there are $p+q-1$ numbers less than n that are not relatively prime to n: these are just p multiples of q and q multiples of p where 0 is a multiple of both q and p. So the probability that a message m is not relatively prime to n is $\frac{p+q-1}{n} < \frac{1}{p} + \frac{1}{q}$, which if p and q both have at least 100 decimal digits, is on the order of 10^{-100} and is too unlikely to worry about. Of course one should be sure $m \neq 0$.

[1] m and n are relatively prime if their only common divisor is 1.

5 The Fast Power Algorithm

Why can we quickly compute $m^e \pmod n$ and $c^d \pmod n$?

Because exponentiation can be done by the fast power algorithm. For example,

$$m^{234} = m^{128+32+16+1} = ((((((m^2)^2)^2)^2)^2)^2)^2 \cdot ((((m^2)^2)^2)^2)^2 \cdot (((m^2)^2)^2)^2 \cdot m \pmod n$$

requires only 10 multiplications. In general a k bit exponent requires at most $2k-2$ multiplications.

6 Uses of Public Keys

The following are some uses of a pair of keys, one public and one private, such that you can encrypt a message with either key and decrypt it with the other, but you cannot find out the private key.

A person announces her public key to the world and keeps her private key private.

If a person X encrypts a message with her private key and sends it to a second person Y, Y knows by the fact that X's public key decrypts the message properly that it comes from X.

If Y encrypts a message with X's public key and sends it to X, only X can decrypt the message, for only X has the necessary private key.

For X and Y to communicate securely, X can encrypt a message first with her private key and then with Y's public key. Y can decrypt the message by applying first Y's private key and then X's public key. Only Y can decrypt the message and Y will know that only X could have sent the message.

A person X can sign a document by encrypting it with his private key. Then anyone can decrypt the document with the public key of X and prove that X signed it.

A problem with document signing is that private keys may be stolen. Thus it becomes important to tell the time a document was signed, so that one can report private keys stolen and make them invalid after a particular time.

Time stamping a document can be done by sending the document to a national time stamping center that adds the time and signs the total result. The national time stamping center must never permit its private key to be stolen, or else documents may be fraudulantly time stamped. The probability of this occuring may be mitigated by having three independent national centers time stamp the document, resting comfortably in the knowledge that it is impossible that all three centers will have their private keys stolen.

7 Euclid's Algorithm

Two natural numbers m and n are 'relatively prime' if their only common divisor is 1.

An important fact about relatively prime numbers m and n is that there exist (possibly negative) integers j and k such that $jm + kn = 1$. A consequence of this is that $jm = 1 \pmod{n}$ and therefore $j \pmod{n}$ is the mod n multiplicative inverse of m, which is written as $j = m^{-1} \pmod{n}$.

We will prove a somewhat more general fact.

The 'greatest common divisor' or gcd of two natural numbers m and n is the largest natural number that divides both m and n exactly. Thus m and n are relatively prime if and only if their gcd is 1. We will prove that if d is the gcd of m and n, then there exist (possibly negative) integers j and k such that $jm + kn = d$.

Euclid's algorithm can be used to find the gcd of two natural numbers m and n. The algorithm is:

1. If $m > n$ switch m and n so that $m \leq n$.
2. Divide n by m to get remainder r. Note that $0 \leq r < m$ and $n = qm + r$ for some natural number q.
3. If $r = 0$ return m as the gcd.
4. Otherwise replace n by r and go to step 1.

The point is that if $r \neq 0$ then m and r have the same gcd as m and n. Since $r < m \leq n$, the numbers keep decreasing. Eventually the algorithm must stop: it will surely stop if the smallest number becomes 1 as then r will be 0 when next computed.

Now consider the set of numbers $S = \{jm + kn \mid j, k \text{ are any integers}\}$. This set is closed under addition and subtraction: the sum and difference of two numbers in S

are also in S. This set is also closed under multiplication by an arbitrary integer: if a number is in S, multiplying it by any integer gives a number in S.

m and n are certainly in S. If m and n are in S at step 1 of the algorithm, then the r computed by step 2 is in S, for $r = n - qm$ for some integer q. So when r replaces n in step 4, the new m and n are in S. Therefore, all the numbers generated by Euclid's algorithm are in S, and the gcd is in S.

Thus we have proved that if d is the gcd of m and n then there are integers j and k such that $jm + kn = d$.

8 Euler's Totient Function

Let n be any non-zero natural number. Let

$$\Phi(n) = \{m \mid 0 \leq m < n \text{ and } m \text{ is relatively prime to } n\}.$$

Then Euler's Totient function, $\phi(n)$ is defined to be the number of elements in $\Phi(n)$. Using $|S|$ to denote the number of elements in a set S, we have $\phi(n) = |\Phi(n)|$.

We want to prove in this section that if m is relatively prime to n, then $m^{\phi(n)} = 1 \pmod{n}$.

$\Phi(n)$ is closed under multiplication mod n, because the product of two numbers relatively prime to n is relatively prime to n. Also, 1 is in $\Phi(n)$.

If m is in $\Phi(n)$, then m and n are relatively prime, and $jm + kn = 1$ for some integers j and k. Therefore $jm = 1 \pmod{n}$ and $j (\text{mod } n)$ is the mod n multiplicative inverse of m. Clearly j and n cannot have a common divisor other than 1, as $jm = 1 \pmod{n}$, so $j (\text{mod } n)$ is also in $\Phi(n)$. We can write $j = m^{-1} (\text{mod } n)$.

Therefore $\Phi(n)$ is a multiplicative group. This means that $\Phi(n)$ is closed under multiplication and under the finding of multiplicative inverses, and 1 is in $\Phi(n)$.

Let m be any element of $\Phi(n)$. Let $G_m = \{m^k \pmod{n} \mid k \text{ is an integer}\}$. Since $G_m \subseteq \Phi(n)$, G_m is finite. So there are distinct integers k_1 and k_2 such that $m^{k_1} = m^{k_2} \pmod{n}$. Without loss of generality let $k_1 < k_2$, and then $m^{k_2 - k_1} = 1 \pmod{n}$. Therefore there is a natural number $k > 0$ such that $m^k = 1$ $(mod\ n)$.

From now on let $k > 0$ be the least natural number such that $m^k = 1$ $(mod\ n)$.

Then G_m has exactly k elements: $m^0 = 1$, m^1, m^2, $\ldots$, m^{k-1}. For suppose that $m^{k_1} = m^{k_2}$ $(mod\ n)$ for natural numbers $k_1 < k_2 < k$ Then $m^{k_2-k_1} = 1 \pmod{n}$ so k would not be the least natural number above 0 such that $m^k = 1 \pmod{n}$.

We will prove that k divides $\phi(n) = |\Phi(n)|$ exactly, so that $jk = \phi(n)$ for some natural number j, and therefore $m^{\phi(n)} = (m^k)^j = 1^j = 1 \pmod{n}$.

G_m is a subgroup of $\Phi(n)$. This means that G_m is closed under multiplication and the finding of multiplicative inverses, and that 1 is in G_m. Since $k = |G_m|$ and $\phi(n) = |\Phi(n)|$, it will suffice to show that if G' is any multiplicative subgroup of a multiplicative group G, then $|G'|$ exactly divides $|G|$. This is a theorem of group theory we will now prove.

For any $x \in G$ let $xG' = \{xg \mid g \in G'\}$ be the 'G'-orbit' of x. If $y \in xG'$, then $y = xg$ for some $g \in G'$, and $x = yg^{-1}$. Since $g^{-1} \in G'$, x is in the G'-orbit of y.

Thus if the G'-orbits of two elements of G have an element in common, the G'-orbits are exactly equal as subsets of G. Since every element of G is in its own G'-orbit, and distinct G'-orbits are disjoint, $|G|$ is the sum of the sizes of the distinct G'-orbits. If we can show that every G'-orbit has size $|G'|$, we will have shown that $|G'|$ exactly divides $|G|$.

If $|xG'| \neq |G'|$ then there must be distinct $g_1, g_2 \in G'$ such that $xg_1 = xg_2$. But multiplying by x^{-1} we get that $g_1 = g_2$ so this is impossible.

9 Finding Large Primes

To use RSA one needs to be able to find very large primes. The algorithm commonly used is due to Rabin and Miller.

Suppose p is a large number that might be prime. There is a way in which a number $a < p$ might be a 'witness' to the fact that p is <u>not</u> prime. Rabin and Miller found a way in which 3/4'ths of all numbers less than a non-prime p were witnesses to the fact that p is not prime. Then by randomly choosing k numbers $a < p$ and checking that none are witnesses to p not being prime, the probability that p is not prime is at most $\frac{1}{4^k}$, which can be made too small to worry about.

It turns out that a large percentage of numbers are prime, so that if p turns out not to be prime, testing the next larger p that is not divisible by primes less than 2000 is a good bet to find a prime.

The Rabin-Miller witness test is as follows:

1. Compute b and m such that $p = 1 + 2^b \cdot m$ where m is odd.
2. Set $j = 0$ and $z = a^m \pmod{p}$.
3. If $z = 1$ or $z = p - 1$ then stop the test and a is not a witness to p not being prime.
4. If $j > 0$ and $z = 1$ then stop the test and a is a witness to p not being prime.
5. Set $j = j + 1$.
6. If $j < b$ and $z \neq p - 1$, set $z = z^2 \pmod{p}$ and go back to step 4.
7. If $z = p - 1$ then stop the test and a is not a witness to p not being prime.
8. If $j = b$ and $z \neq p-1$ then stop the test and a is a witness to p not being prime.

Actually, the probability that a random $a < p$ will be a witness is much higher than 3/4 on average, and it suffices to test about 5 randomly chosen numbers $a < p$. If none is a witness, then p may be assumed to be prime.