Lecture 33

Instructor's Comments: I like to introduce Exponentiation Ciphers first and then tackle RSA - this way students can see the build up and see why one prime is an insecure procedure whereas two primes gives a secure procedure.

Exponentiation Cipher

We begin describing RSA by first explaining exponentiation ciphers. Suppose Alice and Bob want to share a message but there is an eavesdropper (Eve) watching their communications.

Instructor's Comments: Include picture while lecturing.

In an exponentiation cipher, Alice chooses a (large) prime p and an e satisfying

$$1 < e < (p-1) \qquad \text{and} \qquad \gcd(e, p-1) = 1.$$

Alice then makes the pair (e, p) public and computes her private key d satisfying

$$1 < d < (p-1) \qquad \text{and} \qquad ed \equiv 1 \pmod{p-1}$$

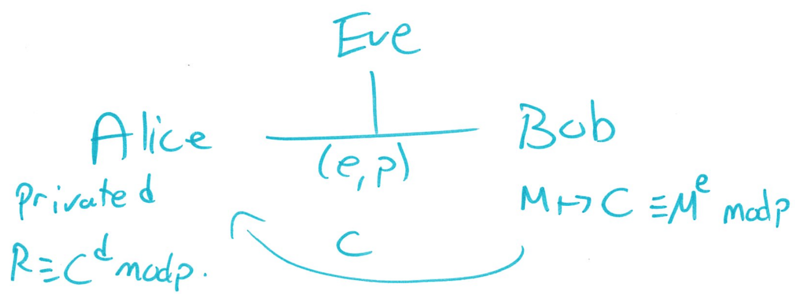
which can be done quickly using the Euclidean Algorithm (the inverse condition above is why we required that $\gcd(e, p-1)$).

To send a message M to Alice, an integer between 0 and $p-1$ inclusive, Bob computes a ciphertext (encrypted message) C satisfying

$$0 \le C < p \qquad \text{and} \qquad C \equiv M^e \pmod{p}.$$

Bob then sends C to Alice.

Alice then computes $R \equiv C^d \pmod{p}$ with $0 \le R < p$.



Instructor's Comments: Include picture - this is the 10 minute mark

Proposition: $R \equiv M \pmod{p}$.

Proof: If $p \mid M$, then all of M, C and R are 0 and the claim follows. So we assume that $p \nmid M$. Recall that $ed \equiv 1 \pmod{p-1}$ and so we have that there exists an integer k such that $ed = 1 + k(p-1)$. Using this, we have

$$\begin{aligned} R &\equiv C^d \pmod{p} \\ &\equiv (M^e)^d \pmod{p} && \text{by definition of } C \\ &\equiv M^{ed} \pmod{p} \\ &\equiv M \pmod{p} && \text{Corollary to F}\ell\text{T since } ed \equiv 1 \pmod{p-1}. \end{aligned}$$

as required ■

Corollary: $R = M$

Proof: By the previous proposition, $R \equiv M \pmod{p}$. Recall that $0 \le M, R < p$ and so the values must be equal. ■

Instructor's Comments: This is the 20 minute mark.

The good news is that this scheme works. However, Eve can compute d just as easily as Alice! Eve knows p, hence knows $p-1$ and can use the Euclidean algorithm to compute d just like Alice. This means our scheme is not secure. To rectify this problem, we include information about two primes.

RSA Alice chooses two (large) distinct primes p and q, computes $n = pq$ and selects any e satisfying

$$1 < e < (p-1)(q-1) \qquad \text{and} \qquad \gcd(e, (p-1)(q-1)) = 1$$

Alice then makes the pair (e, n) public and compute her private key d satisfying

$$1 < d < (p-1)(q-1) \qquad \text{and} \qquad ed \equiv 1 \pmod{(p-1)(q-1)}$$

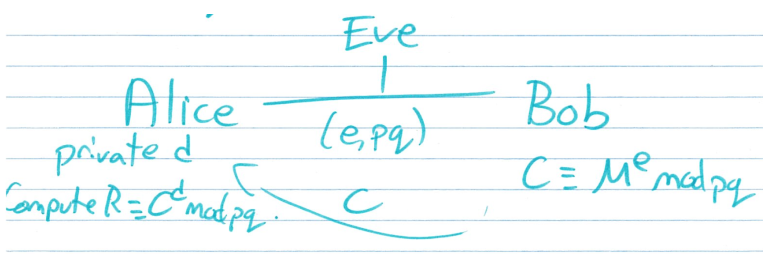
again which can be done quickly using the Euclidean Algorithm (Alice knows p and q and hence knows $(p-1)(q-1)$).

Instructor's Comments: Note that in the textbook (d, n) is the private key pair.

To send a message M to Alice, an integer between 0 and $n-1$ inclusive, Bob computes a ciphertext C satisfying

$$0 \le C < pq \qquad \text{and} \qquad C \equiv M^e \pmod{pq}.$$

Bob then sends C to Alice. Alice then computes $R \equiv C^d \pmod{pq}$ with $0 \le R < pq$.



Instructor's Comments: Include a diagram of what's happening. This is the 30 minute mark.

Proposition: $R = M$.

Proof: Since $ed \equiv 1 \pmod{(p-1)(q-1)}$, transitivity of divisibility tells us that

$$ed \equiv 1 \pmod{p-1} \qquad \text{and} \qquad ed \equiv 1 \pmod{q-1}.$$

Since $\gcd(e,(p-1)(q-1)) = 1$, GCD Prime Factorization (or by definition) tells us that $\gcd(e, p-1) = 1$ and that $\gcd(e, q-1) = 1$. Next, as $C \equiv M^e \pmod{pq}$, Splitting the Modulus states that

$$C \equiv M^e \pmod{p} \qquad \text{and} \qquad C \equiv M^e \pmod{q}$$

Similarly, by Splitting the Modulus, we have

$$R \equiv C^d \pmod{p} \qquad \text{and} \qquad R \equiv C^d \pmod{q}.$$

By the previous proposition applied twice, we have that

$$R \equiv M \pmod{p} \qquad \text{and} \qquad R \equiv M \pmod{q}.$$

Now, an application of the Chinese Remainder Theorem (or Splitting the Modulus), valid since p and q are distinct, gives us that $R \equiv M \pmod{pq}$. Recalling that $0 \le R, M < pq$, we see that $R = M$. ■

Is this scheme more secure? Can Eve compute d? If Eve can compute $(p-1)(q-1)$ then Eve could break RSA. To compute this value given only n (which recall is pq), Eve would need to factor n (or compute $p+q$). Factoring n is a notoriously hard problem and we know of no quick way of doing so. Eve could also break RSA if she could solve the problem of computing M given $M^e \pmod{n}$.

Note: Let ϕ be the Euler Phi Function. This function has the valuation $\phi(n) = (p-1)(q-1)$ when $n = pq$ a product of distinct primes.

Instructor's Comments: This is the 40 minute mark

Handout or Document Camera or Class Exercise

Let $p = 2$, $q = 11$ and $e = 3$

(i) Compute n, $\phi(n)$ and d.

(ii) Compute $C \equiv M^e \pmod{n}$ when $M = 8$ (reduce to least nonnegative C).

(iii) Compute $R \equiv C^d \pmod{n}$ when $C = 6$ (reduce to least nonnegative R).

Solution:

(i) Note $n = 22$, $\phi(n) = (2-1)(11-1) = 10$ and lastly, $3d \equiv 1 \pmod{10}$ and multiplying by 7 gives $d \equiv 7 \pmod{10}$. Hence $d = 7$.

(ii) Note that

$$\begin{aligned} C &\equiv M^e \pmod{22} \\ &\equiv 8^3 \pmod{22} \\ &\equiv 8 \cdot 64 \pmod{22} \\ &\equiv 8 \cdot (-2) \pmod{22} \\ &\equiv -16 \pmod{22} \\ &\equiv 6 \pmod{22} \end{aligned}$$

(iii) The quick way to solve this is to recall the RSA theorem and hence $M = 8$. The long way is to do the following:

$$\begin{aligned} R &\equiv C^d \pmod{22} \\ &\equiv 6^7 \pmod{22} \\ &\equiv 6 \cdot (6^3)^2 \pmod{22} \\ &\equiv 6 \cdot (216)^2 \pmod{22} \\ &\equiv 6 \cdot (-4)^2 \pmod{22} \\ &\equiv 6 \cdot 16 \pmod{22} \\ &\equiv 6 \cdot (-6) \pmod{22} \\ &\equiv -36 \pmod{22} \\ &\equiv 8 \pmod{22} \end{aligned}$$

Food for thought:

(i) How does Alice choose primes p and q? (Answer: Randomly choose odd numbers! If p and q are 100 digit primes, then choosing 100 gives you more than a 50% chance that you have a prime - can check using primality tests).

(ii) What if Eve wasn't just a passive eavesdropper? What if Eve could change the public key information before it reaches Bob? (This involves using certificates).

(iii) What are some advantages of RSA? (Believed to be secure, uses the same hardware for encryption and decryption, computations can be done quickly using a square and multiply algorithm).