Discrete Mathematics **U. Waterloo ECE 103, Spring 2010**
Ashwin Nayak **June 14, 2010**

Encryption

These are supplementary notes on encryption schemes.

Private key encryption

Here, we see a private key encryption scheme that is completely secure, as long as the key used is kept secret.

The messages are represented by integers M, with $0 \leq M < n$, for some positive integer n. The key k is an arbitrary integer k such that $0 \leq k < n$, chosen jointly by the sender and the receiver, and is known only to them.

Ecryption: The sender computes $C \equiv M + k \pmod{n}$, with $0 \leq C < n$, i.e., it is the remainder when $M + k$ is divided by n. She then sends the ciphertext C to the receiver.

Decryption: The receiver computes $D \equiv C - k \pmod{n}$, with $0 \leq D < n$.

Since both D, M lie in the interval $[0, n)$, and $D \equiv C - k \equiv M + k - k \equiv \pmod{n}$, we have $D = M$. In other words, the receiver correctly decrypts the ciphertext.

As long as she does not know the key, any eavesdropper who intercepts the ciphertext C will not get any information about the message M. The ciphertext C is consistent with every possible value for the message in the range $[0, n)$: for every value $M' \in \{0, 1, \ldots, n-1\}$, there is a possible value k' for the key so that $M' + k' \equiv C \pmod{n}$.

This kind of a scheme is said to be *information-theoretically secure*. A major disadvantage of such schemes is the need for the sender and the receiver to agree upon a secret key before communicating sensitive data to each other. If a million customers wish to look up their bank balances online, they would each have to establish a separate key with the bank. With current technology, this requires the two parties to physically meet to establish the key. Moreover, the key may only be used to send one message. Reusing a key compromises its secrecy. Public key cryptography overcomes several of these disadvantages.

RSA encryption

In this section, we review two aspects of the RSA encryption scheme. First, we prove that the receiver decrypts the ciphertext correctly. This is an alternative proof of Theorem 5.2.1 in the text book, using only the number theory we have learnt in class.

Recall the following property of divisibility.

Theorem 1 *If $a|c$, $b|c$, and $\gcd(a, b) = 1$, then $(ab)|c$.*

In an RSA encryption scheme, we have $n = pq$, where p, q are distinct primes. The public key is (e, n), where $\gcd(e, \phi(n)) = 1$, with $\phi(n) = (p-1)(q-1)$ and $0 \leq e < \phi(n)$. The private key is (d, n), where $ed \equiv 1 \pmod{\phi(n)}$, and $0 \leq d < \phi(n)$. The ciphertext C corresponding to a message M in the range $[0, n)$ is such that $C \equiv M^e \pmod{n}$, with $0 \leq C < n$. The receiver decrypts this as $D \equiv C^d \pmod{n}$, with $0 \leq D < n$.

Theorem 2 $D = M$.

Proof : It suffices to show that $D \equiv M \pmod{n}$, since both the numbers lie in the range $[0, n)$.

Since $n = pq$, and p, q are distinct primes (meaning $\gcd(p, q) = 1$), by Theorem 1, it suffices to show that $p|(D - M)$, and $q|(D - M)$.

We only show that $p|(D - M)$, as the proof for divisibility by q is similar.

We have $D \equiv C^d \equiv M^{ed} \pmod{pq}$, i.e., $(pq)|(D - M^{ed})$. This implies that $p|(D - M^{ed})$, i.e., $D \equiv M^{ed} \pmod{p}$.

If $p|M$, then $D \equiv 0 \equiv M \pmod{p}$.

If $p \not| M$, then by the Fermat Little Theorem, $M^{p-1} \equiv 1 \pmod{p}$. Since $ed \equiv 1 \pmod{(p-1)(q-1)}$, we have $ed = k(p-1)(q-1) + 1$, for some integer k. So $M^{ed} = M \times M^{k(p-1)(q-1)} \equiv M \pmod{p}$.

In either case, we have $D \equiv M \pmod{p}$. Similarly we have $q|(D - M)$, and as mentioned above, this implies that $D = M$. ■

Second, we review how the sender and the receiver encrypt and decrypt. Both these operations involve exponentiation modulo n. To do this efficiently, we use the recursive exponentiation algorithm we learnt in class. The only difference is that we reduce all the intermediate results modulo n so that the numbers with which we compute do not blow up in size.

Example 1 *Encrypt* $M = 2$ *with the public key* $(35, 323)$.

Solution : The following table summarizes our calculations. Let $a = 2$, and b denote the value returned by the recursive call to Power in one step, modulo 323.

Step	n	b	calculation $\pmod{323}$	value $\pmod{323}$
1	35	a^{17}	$2 \times (257)^2 \equiv 2 \times 157$	314
2	17	a^8	$2 \times (256)^2 \equiv 2 \times 290$	257
3	8	a^4	$(16)^2$	256
4	4	a^2	4^2	16
4	2	a	2^2	4
4	1			2

The ciphertext is 314. ■