6.875J/18.425J Cryptography and Cryptanalysis	September 12, 2001
Lecture 3	
Instructor: Anna Lysyanskaya	*Scribed by: Jennifer Mulligan*

Lecture Summary

1. Recap of Lecture 2:
   i. notation
   ii. definition of security for a public key Cryptosystem
2. Quadratic Residuosity Assumption

1 Notation

Let A denote an algorithm. Let $A(\cdot)$ denote the fact that A has one input. $A(\cdot,\cdot)$ denotes the fact that A has two inputs.

$A(x)$ is a well-defined quantity if A is deterministic.

$A(x)$ defines a probability distribution if A is probabalistic. More precisely: Let $A'(\cdot,\cdot)$ be the deterministic algorithm such that $A'(x,R)$ is equal to $A(x)$ with the random tape R. Then $A(x)$ is the distribution induced by picking R uniformly at random and running $A'(x,R)$.

$y \leftarrow A(x)$ corresponds to choosing y from the distribution induced by $A(x)$.

EXAMPLE 1
$((x,y) \leftarrow A(3); z \leftarrow B(y))$ means that A was run on the input 3, producing values x and y for output. Next B was run with input y and produced output z.

EXAMPLE 2
Let $B(x)$ be a boolean function of variable x.
To denote "Probability that $B(y)$ is true, given that y is generated by A being run on x," we write $Pr[y \leftarrow A(x) : B(y)]$

EXAMPLE 3
Let us formalize a statement such as "factoring RSA moduli is hard." What does this mean? First, it means that someone chose n at random. Then this n is given to the adversary. Then the adversary tries to factor n and produces a candidate factor p'. We wish to limit the probability that p' is a non-trivial factor of n, $\forall ppt A_k$.
First, let us repeat this in English:

$Pr[$ 1. n gets chosen in some way;
2. n is given to the adversary and the adversary ouputs a candidate factor p' of n
: $p' \neq 1$ and $p' \neq n] \leq$ negligible function

And now let us rewrite this using our notation:

Let $PRIMES_k$ denote prime numbers of length k.
$\forall ppt A_k$, $\exists$ negligeble function f such that.
$Pr[p \leftarrow PRIMES_k; q \leftarrow PRIMES_k; n = p \cdot q \; p' = A_k(n)$
$: p' \neq 1$ and $p' \neq n$ and $p'|n] \leq f(k)$

2 Definition of Security for Public Key Cryptosystems

Algorithms that Comprise a Cryptosystem

1. G - Key Generation Algorithm
2. E - Encryption Algorithm
3. D - Decryption Algorithm

Definition of Security

In English, the definition of security that seems reasonable is: "Deciding the encrypted bit is hard for a randomly chosen key pair for all probabalistic polynomial time adversaries."

Expanded, but still in English, what we want is the following: a key pair (PK, SK) is chosen using algorithm G; a bit b is chosen at random, and encrypted under PK using algorithm E; the resulting ciphertext c is given to the adversary; the adversary's guess b' coincides with the encrypted bit b with probability only negligibly better than 1/2.

Or more precisely:

$\forall ppt\{A_k\}\exists$ negligible function $f(x)$ such that $\forall k$

$Pr[(PK, SK) \leftarrow G(1^k); b \leftarrow 0, 1; c \leftarrow E(b, PK); b' \leftarrow A_k(c, PK)$
$: b' = b] \leq \frac{1}{2} + f(k)$

3 Quadratic Residuosity Assumption

Definition of the Legendre Symbol:

Let p be a prime number.

$$\left(\frac{a}{p}\right) \doteq \begin{cases} 0: & \text{if } GCD(a,p) \neq 1 \\ 1: & \text{if } GCD(a,p) = 1 \text{ and } a \text{ is a square mod } p \\ -1: & \text{if } GCD(a,p) = 1 \text{ and } a \text{ is not a square mod } p \end{cases}$$

Definition of Jacobi Symbol for RSA Moduli:

$$\left(\frac{a}{n}\right) \doteq \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$$

Quadratic Residuosity Assumption:

If n is an RSA modulus chosen as random, and a random $a \in \mathbb{N}_n^*$, with Jacobi symbol 1, then you can't tell whether a has a square root mod n or not.

Using our notation, the assumption is as follows:

Let $J_1(n)$ denote the selection of a random element of $\mathbb{Z}_n^*$ mod n with Jacobi Symbol 1.

Let $QC(a, n)$ denote the quadratic character of a modulo n. That is to say, $QC(a, n) =$ "square" if a is a square and $QC(a, n) =$ "non-square" otherwise.

$\forall ppt\{A_k\}\exists$ negligible function f such that $\forall k$:

$Pr[p \leftarrow PRIMES_k; q \leftarrow PRIMES_k; a \leftarrow J_1(p*q); b' \leftarrow A_k(n, a)$
$: b = QC(a, n)] \leq \frac{1}{2} + f(k)$

By the Chinese Remainder Theorem we know that there exist a_1 and a_2 such that

$$a = a_1 \bmod p$$

$$a = a_2 \bmod q$$

4 Useful Number-Theoretic Facts

The term "square" can be used interchangeably with the term "quadratic residue" throughout.

Fact 0 (Fermat's little theorem): If p is prime, and a is relatively prime to p, then $a^p \equiv a \bmod p$.

Fact 1: $\mathbb{Z}_p^*$ is cyclic, i.e. there exists an element $g \in \mathbb{Z}_p^*$ such that for all elements $a \in \mathbb{Z}_p^*$ there exists a unique number $0 \leq u \leq p-1$ such that $a \equiv g^u \bmod p$. Such g is called a *generator* mod$p$.

Fact 2 (The Chinese Remainder Theorem): Let $m_1, \ldots, m_k$ be pairwise relatively prime integers. That is, $gcd(m_i, m_j) = 1$ for all $1 \leq i \leq j \leq k$. Let the values $a_i \in \mathbb{Z}_{m_i}$ be given for $1 \leq i \leq k$. Let $m = \prod m_i$. There exists a unique $a \in \mathbb{Z}_m$ such that $a \equiv a_i \bmod m_i$ for all i. Furthermore there is an $O(k\ell^2)$ time algorithm to compute a given $a_1, \ldots, a_k$, $m_1, \ldots, m_k$, where $\ell = \max(|m_i|)$.

We won't give a proof of Facts 0, 1 and 2; see, for example, Goldwasser-Bellare's lecture notes for reference.

Fact 3: If $p > 2$ is prime, and g is a generator mod$p$, then g cannot be a square mod$p$. That is, for all $h \in \mathbb{Z}_p^*$, it is not the case that $h^2 \equiv g \bmod p$.

Proof: Suppose $\exists h$ such that $h^2 = g$, then $h^{p-1} = 1 (\bmod p)$ by Fermats Little Theorem, and so $(h^2)^{\frac{p-1}{2}} = 1 (\bmod p)$. Consequently $g^{\frac{p-1}{2}} = 1 (\bmod p)$ but this is a contradiction because g is a generator. (Exercise: Why can't it be that for some $1 \leq u < p-1$, $g^u \equiv 1 \bmod n$ if g is a generator?)

Fact 4: Let $p > 2$ be a prime. Let g be a generator mod$p$. Let $a \equiv g^u \bmod p$ be given. a is a square if and only if u is even.

Proof: Assume u is even, then $a = g^{2v} = g^{v2} \bmod p$ and a is obviously a quadratic residue.

Assume a is a quadratic residue. Suppose that u is odd, $u = 2v + 1$. Since a is a quadratic residue, $g^{2v+1} = b^2 \bmod p$ for some b.

$$g = \frac{b^2}{g^{2v}} \bmod p$$

$$= (\frac{b}{g^v})^2 \bmod p$$

but then g would be a quadratic residue which contradicts Fact 3.

Fact 5: Let $p > 2$ be a prime. Exactly one half of the elements of $\mathbb{Z}_p^*$ are quadratic residues mod$p$.

Proof: This is simply a corollary to Fact 4.

Fact 6: Let $p > 2$ be a prime. Let a be a square mod$p$. Then a has exactly two square roots mod$p$.

Proof: First, let us show that a has at least two square roots: By Fact 4, $a \equiv g^{2v}$ for some generator g and some number $1 \le v \le (p-1)/2$. Consider g^v and $g^{(p-1)/2+v}$. Observe that they must be distinct. Also observe that they are both square roots of a. Now, we must show that no number has more than two square roots modulo p. For that, we do a counting argument: by Fact 5, there are $(p-1)/2$ quadratic residues. We just saw that each of them has at least 2 square roots. That brings us to $p-1$ elememts accounted for. There is no more room for any other element to have any other square root.

Fact 7: Let $p > 2$ be a prime. Then 1 is a square mod$p$ and its only square roots are 1 and -1 mod p.

Proof: Fact 7 is simply a corollary of Fact 6.

Fact 8: Let p be a prime. Then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Proof: Let g be a generator. Let $a \equiv g^u \bmod p$, $b \equiv g^v \bmod p$. By Fact 4, $\left(\frac{ab}{p}\right) = 1$ if and only if $u + v$ is even, otherwise it's -1. On the other hand, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1$ also if and only if $u + v$ is even, otherwise it's -1. Fact 6 follows.

Fact 9: The Legendre Symbol is computed by the following algorithm:

Test $p|a$, if p does divide a output 0, otherwise output $a^{\frac{p-1}{2}} \bmod p$

Proof: Case 1: a is a square. By Fact 4 $\exists v$ such that $a = g^{2v} \bmod p$

$$a^{\frac{p-1}{2}} = (g^{2v})^{\frac{p-1}{2}} = g^{v(p-1)} = 1 \bmod p$$

Thus we have shown that if a is a square, the Legendre Symbol is computed correctly.

Case 2: a is not a square. Then by Fact 4, $a \equiv g^{2v+1} \bmod p$. Therefore, $a^{(p-1)/2} \equiv (g^v)^{p-1} g^{(p-1)/2} \bmod p$. By Fermat's little theorem, we know that $(g^v)^{p-1} \equiv 1$. What about $g^{(p-1)/2} \bmod p$? First, observe that it is a square root of 1, since $g^{p-1} \equiv 1$. Now, notice that since g is a generator, it cannot be equal to 1. 1 has only two square roots, and by Fact 7 they are 1 and -1. We've ruled out 1, so it must be -1.

Fact 10: a is a quadratic residue mod $n = p_1 p_2$ if and only if a_1 is a square modp_1 and a_2 is a square modp_2, where $p_1 > 2$ and $p_2 > 2$ are primes.

Proof: Let us first show the $\Rightarrow$ direction. Assume a is a quadratic residue. We need to show that a_1 and a_2 are also quadratic residues.

$\exists b$ such that $b^2 = a \bmod n$.
Let $b_1 = b \bmod p_1$ and $b2 = b \bmod p_2$.

$$b_1^2 = b^2 = a = a_1 \bmod p_1$$

. Therefore, a_1 is a square. Similarly for b_2, which proves that a_2 is a quadratic residue as well.

Assume that a_1 and a_2 are quadratic residues.
$\exists b_1, b_2$ such that $a_1 = b_1^2 \bmod p$ and $a_2 = b_2^2 \bmod q$. Then by the Chinese Remainder Theorem, $\exists b$ such that $b = b_1 \bmod p$ and $b = b_2 \bmod q$.

$$b^2 = a_1 \bmod p$$

$$b^2 = a_2 \bmod p$$

Therefore since a is unique, $b^2 = a \bmod n$ by the Chinese Remainder Theorem.
Fact 11: Let n be an RSA modulus (i.e., $n = p_1 p_2$, where $p_1 > 2$ and $p_2 > 2$ are primes). Exactly one quarter of the elements of $\mathbb{Z}_n^*$ are quadratic residues.

Proof: Easy to see by combining Fact 10 with Fact 5.
Fact 12: Let $n = pq$ be an RSA modulus. Exactly half of the elements of $\mathbb{Z}_n^*$ have Jacobi Symbol 1.

Proof: This is obtained by a counting argument. Consider $a \in \mathbb{Z}_p^*$, $b \in \mathbb{Z}_q^*$. By the Chinese Remainder Theorem, there is a unique element c that corresponds to them. Moreover, by definition, $\left(\frac{c}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{q}\right)$. There are four possibilities. Case 1: $\left(\frac{a}{p}\right) = 1$, $\left(\frac{b}{q}\right) = 1$, and so $\left(\frac{c}{n}\right) = 1$. Case 2: $\left(\frac{a}{p}\right) = 1$, $\left(\frac{b}{q}\right) = -1$, and so $\left(\frac{c}{n}\right) = -1$. Case 3: $\left(\frac{a}{p}\right) = -1$, $\left(\frac{b}{q}\right) = 1$, and so $\left(\frac{c}{n}\right) = -1$. Case 4: $\left(\frac{a}{p}\right) = -1$, $\left(\frac{b}{q}\right) = -1$, and so $\left(\frac{c}{n}\right) = 1$. By Fact 5, it is easy to see that exactly one quarter of c's correspond to each of these cases.
Fact 13: Let n be an RSA modulus. Let $J_1(n)$ denote the set of elements of $\mathbb{Z}_n^* \bmod n$ with Jacobi Symbol 1. Exactly half of the elements of $J_1(n)$ are squares.

Proof: This follows from the proof of Fact 12.
Fact 14: Let $n = pq$ be an RSA modulus. One can efficiently determine the quadratic character of any $a \in \mathbb{Z}_n^*$ given the factorization of n.

Proof: For example, this can be done by computing $\left(\frac{a}{p}\right)$ and $\left(\frac{a}{q}\right)$ and verifying that these are 1. By Fact 10 this gives the right answer, and by Fact 9 this can be done efficiently.
Fact 15: Let n be an RSA modulus. For any $a \in \mathbb{Z}_n^*$, one can efficiently compute $\left(\frac{a}{n}\right)$ *without the factorization of* n.

Proof: We will omit the proof, but you can find it in GB lecture notes.

Don't confuse the Jacobi symbol modulo n and the quadratic character modulo n. Fact 15 tells us that the Jacobi symbol can be computed even without the factorization of n, while the quadratic character modulo n is something that we hope can *only* be computed if the factorization of n is known.