CSE 599b: Cryptography **(Winter 2006)**

Lecture 13: Public Key Encryption Schemes

15 February 2006

Lecturer: Paul Beame *Scribe: Paul Beame*

RSA is not the only way to build public key encryption. We consider some of the other candidates.

1 Blum Squaring

Recall the collection of functions $\{Blum_N : QR_N \rightarrow QR_N\}$ were $Blum_N = x^N \mod N$ for so-called *Blum integers* N that are products of two distinct primes congruent to $3 \mod 4$ are candidate one-way functions. As we mentioned earlier, inverting for algorithms for $Blum_N$ yield algorithms for factoring N.

We now show that for $N = pq$, $p \neq q$ prime, $p, q \equiv 3 \pmod 4$, the pair (p, q) of factors of N forms trapdoor for $Blum_N$.

Consider the non-zero integers mod p, $\mathbb{Z}_p^*$. Recall that $\mathbb{Z}_p^*$ is cyclic, equalling $\{1, g, g^2, \ldots, g^{p-2}\}$ for some $g \in \mathbb{Z}_p^*$. QR_p consists of the set of even powers of g, g^{2k} for some integer k. Therefore if $h \in QR_p$ then $h^{(p-1)/2} = (g^{2k})^{(p-1)/2} \equiv 1 \pmod p$. If $h = q^{2k+1}$ then $h^{(p-1)/2} = (g^{2k+1})^{(p-1)/2} = g^{(p-1)/2} \equiv -1 \pmod p$.

Now suppose that $p = 4m + 3$; in this case in particular $(-1)^{(p-1)/2} = (-1)^{2m+1} = -1$ and thus -1 is not a quadratic residue. Moreover, suppose now that $a \in QR_p$. Then $a^{(p-1)/2} \equiv 1 \pmod p$. Thus $a^{2m+1} \equiv 1 \pmod p$ and thus $a^{2m+2} \equiv a \pmod p$. In particular, this means that if $b_p = a^{m+1} \mod p = a^{(p+1)/4} \mod p$ then $b_p^2 \equiv (a^{2m+2}) \equiv a \pmod p$. Thus b_p is a square root of a modulo p.

By similar computation define $b_q = a^{(q+1)/4} \pmod q$. Then $b_q^2 \equiv a \pmod q$.

We now have square roots $\pm b_p$ and $\pm b_q$ of a modulo p and q respectively. Since -1 is not in QR_p, only one of b_p or $-b_p$ will be in QR_p; similarly, only one of b_q or $-b_q$ will be in QR_q. Assume without loss of generality that the elements of QR_p and QR_q are b_p and b_q respectively.

We now use Chinese remaindering to find a $b \in QR_N$ such that $b^2 \equiv a \pmod N$.

Chinese Remaindering

Since $p \neq q$ we can use Euclid's algorithm to produce $u_q = q^{-1} \mod p$ and $u_p = p^{-1} \mod q$. Thus $qu_q \equiv 1 \pmod p$ and $pu_p \equiv 1 \pmod q$.

Now let $b = b_p q u_q + b_q p u_p$. Then $b^2 \mod p = (b_p q u_q)^2 \mod p = b_p^2 \mod p = a \mod p$ and $b^2 \mod q = (b_q p u_p)^2 \mod q = b_q^2 \mod p = a \mod q$. Therefore $b^2 \equiv a \pmod N$. Moreover b is itself in QR_N since $b \mod p$ is in QR_p and $b \mod q$ is in QR_q.

2 El Gamal Encryption

Because there is no known trapdoor that allows one to compute the discrete log effciently, the constructions using the difficulty of computing discrete logarithms are different from the general constructions we have seen, although it is inspired by the basic probabilistic encryption method of Goldwasser and Micali.

The El Gamal encryption scheme is defined over any cyclic group $G = \{1, g, g^2, \ldots, g^{q-1}\}$ for which group product and inverses are efficiently computable. In general for this scheme it is best to have the size of G, q, to be prime.

A typical choice of the group G is the following: Let p be a prime of the form $2q + 1$ for q a prime. Instead of using the group $\mathbb{Z}_p^* = \{1, g, g^2, \ldots, g^{p-2}\}$, the group G will be $QR_p = \{1, g^2, g^4, \ldots, g^{p-3}\} = \{1, h, h^2, \ldots, h^{q-1}\}$ for $h = g^2$. (We will see that choosing $\mathbb{Z}_p^*$ would not be a good idea.)

Typically we have described encryption schemes involving an infinite family of schemes parametrized by a key length parameter. We could do that if we specialized the El Gamal scheme to the groups QR_p as above. However, for more generality we simply describe it for each group G independently.

Definition 2.1. *For a cyclic group G of order q with generator g and efficiently computable group product and inverse, the public key encryption scheme El Gamal$_{(G,g)}$ is defined by the following:*

- *The key generation algorithm $\mathcal{G}$ produces a pair (e, d) by choosing y uniformly at random from $\mathbb{Z}_q$, computes $Y = g^y$ and sets $e = (G, q, Y)$ and $d = (G, g, y)$. (Note that since multiplication in G is efficiently computable, exponentiation in G is also efficiently computable using repeated squaring.)*

- *Given a message M interpreted as an element of G, the encryption algorithm $\mathcal{E}_e(M)$ is computed by choosing r uniformly at random from $\mathcal{Z}_q$ and returning the pair $(g^r, Y^r M)$.*

- *Given a ciphertext (R, Z) for $R, Z \in G$, the decryption algorithm D_d on input R and Z, returns ZR^{-y}. (By definition $R = g^r$ for some r and $Z = Y^r M = g^{yr} M$, so $ZR^{-y} = g^{yr} M g^{-ry} = M$.)*

Intuitively, the security of the El Gamal scheme is related to the Diffie-Hellman scheme, since an adversary has access to the public key and the ciphertext which includes $R = g^r$, $Y = g^y$, and can recover the message from the ciphertext given g^{ry}.

Definition 2.2. *The Decision Diffie-Hellman (DDH) Assumption for cyclic group G of order q and generator g is that it is computationally hard for an algorithm to distinguish distributions (g^a, g^b, g^{ab}) for random $a, b \in \mathbb{Z}_q$ from (g^a, g^b, g^z) for random $a, b, z \in \mathbb{Z}_q$.*

(Again we have ignored our usual asymptotic notation and describe this for an individual group. For an infinite family of groups parametrized by their size we could make 'computationally hard' be our usual notion of computational indistinguishable.)

Theorem 2.3. *El Gamal$_{(G,g)}$ is IND-CPA secure if and only if DDH$_{(G,g)}$ holds.*

Before we go into the proof we see why we do not want to choose the group G in the El Gamal scheme to be $\mathbb{Z}_p^*$. Consider DDH for $\mathbb{Z}_p^*$. Above we noted that given an $A = g^a$ we can tell whether a is even or odd by computing $A^{(p-1)/2}$ and observing whether we obtain 1 or -1. Now given $A = g^a$, $B = g^b$, if both a and b are odd then ab is odd so for a random $z \in \mathbb{Z}_{p-1}$, g^z can be distinguished from g^{ab} with probability at least 1/2. Similar if either a or b is even then ab is even and again g^z can be distinguished from g^{ab} with probability at least 1/2. Thus $DDH_{\mathbb{Z}_p^*}$ is false. It is easy to see that the same reasoning holds if the order of the group q has any small prime factor.

We now prove Theorem 2.3.

Proof. We consider the following characterization of IND-CPA security for a public key encryption scheme: For any time-bounded adversary T and message construction algorithm $\mathcal{M}$, the probability that for (e, d) output by $\mathcal{G}$, message M output by $\mathcal{M}(e)$ and a random $M' \neq M$, the probability that $T(e, \mathcal{E}_e(M), M) = 1$ differs by at most ϵ from the probability that $T(e, \mathcal{E}_e(M'), M) = 1$.

Now specializing this to the El Gamal scheme for G and g this definition is equivalent to saying that for y randomly chosen from $\mathbb{Z}_q$ and $Y = g^y$, message M chosen as $\mathcal{M}(Y)$, random message M', and r randomly chosen from $\mathbb{Z}_q$, the probability that $T(g, Y, R, Z, M) = T(g, g^y, g^r, g^{yr}M, M) = 1$ differs by at most ϵ from the probability that $T(g, g^y, g^r, g^{yr}M', M) = 1$. The only difference in these two cases is that the fourth input to A is $g^{yr}M'$ versus $g^{yr}M$.

Suppose that $\text{DDH}_{(G,g)}$ fails, that is there is an algorithm D that takes inputs (A, B, C) in G^3 and can distinguish distributions (g^a, g^b, g^{ab}) from (g^a, g^b, g^z) for random $a, b \in \mathcal{Z}_q$, and $z \neq ab$ with probability more than ϵ. Define algorithm $\mathcal{M}(Y)$ to output some fixed message M ignoring Y. Define algorithm T that on input (g, Y, R, Z, M) computes $A = R$, $B = Y$ and $C = Z/M$. Observe that if (R, Z) is the El Gamal encryption of M then $C = g^{ry}$ for $A = g^r$ and $B = g^y$. Since r and y are randomly chosen in $\mathbb{Z}_q$, the input distribution of (A, B, C) looks like (g^a, g^b, g^{ab}) for random a, b. However, for a random M', C will be of the form g^z for random z. Therefore the algorithm T will distinguish this with probability more than ϵ.

Conversely, suppose that the IND-CPA security of $\text{El Gamal}_{(G,g)}$ fails, i.e. there is a time-bounded algorithm T such that for r, y randomly chosen and M' randomly chosen the probability that $T(g, g^y, g^r, g^{yr}M, M) = 1$ is more than ϵ larger than the probability that $T(g, g^y, g^r, g^{yr}M', M) = 1$.

Now suppose that we have inputs (A, B, C) for $A = g^a$, $B = g^b$ and we want to determine if $C = g^{ab}$. Define an algorithm D that on input (A, B, C):

1. Chooses a random $w \in \mathbb{Z}_q$ and computes $Y = B^w = g^{bw}$.
2. Chooses random $s, t \in \mathbb{Z}_q$, chooses $M = \mathcal{M}(Y)$ and computes $R = A^s g^t = g^{as+t}$ and $Z = C^{sw}Y^t M = g^{zsw+bwt}M$ for $C = g^z$ and passes the result to T. D outputs what T outputs.

Now, by construction Y is a uniformly random element of G as in the El Gamal key generation, R is also a random element of G, and (R, Z) is an encryption of M if and only if $zsw+bwt = bw(as+t)$ which is true if and only if $z = ab$. Furthermore for $C = g^z$ for a random z then Z is a uniformly random element of G that is independent of R and thus (R, Z) is an encryption of a random $M' \in G$.

Therefore the difference in the probability that D outputs 1 in the two cases is precisely the difference in the probability that T outputs 1 in these cases when is more than ϵ and thuse the $DDH_{(G,g)}$ assumption fails. □

The El Gamal scheme will be the basis for the IND-CCA2 secure public key Cramer-Shoup encryption scheme that we define later but so far it is just as insecure under this kind of attack as all our previous constructions. In order to define this scheme we will need cryptographic hash functions which we define next time.