ICS 280: Introduction to Cryptography 1/27/2004

Handout 1: Homework 1

1 Can functions which have small ranges be One Way?

Let's show that a range of one way function cannot be bounded by a polynomial in the security parameter. In other words, we want to show that if f is a OWF and $R_k = \{f(x)|x \in \{0,1\}^k\}$, than there is no polynomial $p(k)$, s.t. $|R_k| \leq p(k)$ for all sufficiently large k.

1.1

Note that if f on domain $\{0,1\}^k$ has range of size $|R_k| \leq p(k)$ then the average size of a preimage $N_y = f^{-1}(y) = \{x \in \{0,1\}^k \mid f(x) = y\}$ of any element $y \in R_k$, is at least $2^k/p(k)$. (We are averaging over y's in R_k.)

Therefore, consider first a OWF candidate function f which spreads its outputs evenly, in the sense that for every $y \in R_k$ we have $|N_y| \geq \lfloor 2^k/p(k) \rfloor$.

Argue that such f cannot be a OWF by constructing a PPT algorithm A which takes time about $S_k + E_k$, where S_k is the time to sample an element in $\{0,1\}^k$ and E_k is the time to evaluate function f on an input in $\{0,1\}^k$, s.t. A's advantage in inverting f is about $1/(p(k))$.

1.2

Now consider any function f with a polynomially bounded range. Take any k big enough so that $|R_k| \leq p(k)$. Note that sets $N_1, N_2, ..., N_{|R_k|}$ partition the whole domain $\{0,1\}^k$. Note that there must exist i s.t. $N_i > 2^k/p(k)$. Show a PPT algorithm running in time about $S_k + E_k$, whose advantage in inverting f is at least $1/(p(k))^2$.

1.3

Show how to boost this advantage: Construct a PPT algorithm running in time $p(k) * (S_k + E_k)$ whose advantage in inverting f is about $1/e * 1/p(k)$. (Use the fact that $(1 - 1/k)^k \approx 1/e$.)

Note: Our ability to boost the adversarial advantage by increasing the adversary's running time leads to the realization that a quality of an attack algorithm can be measured as $s_A(k) = Time_A(k) * Adv_A(k)$. Note that for the two attack algorithms, for A of sections 1.2 and A' of section 1.3, we have $s_A(k) = \Theta(s_{A'}(k))$.

1.4

Show that the same algorithm as in (1.2) in fact already has a much higher success probability, namely $Adv_A(k) \geq 1/(2p(k))$. It might help to divide sets N_i into "small" and "large"

by considering N_i small if $|N_i| < 2^k/(2p(k))$, and large otherwise, and showing that at least half the points in the domain are in large N_i's.

2 Consequences of Indistinguishability for an Encryption Scheme

Let's see if the definition of security of a (symmetric) encryption scheme $(KGen, Enc, Dec)$ in terms of *indistinguishability of ciphertexts*, which is the defintion we discussed in class, is powerful enough to imply other natural security properties of encryption.

First let's recall the definition we had in class:

Definition 1 *Encryption scheme* $(KGen, Enc, Dec)$ *is* indistinguishable *if for every probabilistic polynomial time algorithm* A *and every polynomial* $l(n)$*, there is a negligible function* $\epsilon(n)$ *s.t. for all* n*, and all* $m_0, m_1 \in \{0,1\}^{l(n)}$*, we have*

$$Adv_A(n) = |Pr[A(m_0, m_1, c) = 1 \mid k \leftarrow KGen(1^n); c \leftarrow Enc(k, m_1)] - \\ -Pr[A(m_0, m_1, c) = 1 \mid k \leftarrow KGen(1^n); c \leftarrow Enc(k, m_0)]| \leq \epsilon(n)$$

In other words, A cannot tell between an encryption of m_0 and an encryption of m_1, for *any* two polynomially-long messages m_0 and m_1.

2.1 Hardness of decrypting a random ciphertext

If an encryption scheme $(KGen, Enc, Dec)$ is secure in the sense of indistinguishability of ciphertexts, is it also secure in the sense that a ciphertext of a random message is hard to decrypt without a key? First propose a formal definition of an encryption scheme for which it is infeasible for an efficient adversary (who does not have an encryption key) to decrypt a ciphertext of a random message.

Then either prove that an indistinguishable encryption scheme must be secure in the sense of resistance to decryption, or give a counterexample which shows that this new security property is strictly stronger.

2.2 Hardness of decryption (cont.)

Consider also the opposite question: If a cipher is secure in the new sense, then must it be secure in the sense of indistinguishability? Either prove that it must be or show a counterexample.

2.3 Hardness of telling any bit information on a message

If an encryption scheme $(KGen, Enc, Dec)$ is secure in the sense of indistinguishability of ciphertexts, is it also secure in the following sense: Given a ciphertext of a random message $m \in \{0,1\}^k$ where k is the security parameter, is it infeasible for an adversary to decide with a probability which is significantly (i.e. non-negligibly) higher than $1/2$, on the input of the ciphertext only, if some one-bit information function $B(m)$ is 0 or 1, for a random m?

A one-bit information function is a function $B : \{0,1\}^* \rightarrow \{0,1\}$ s.t. for every k, for a random m in $\{0,1\}^k$, the probability $Pr[B(m) = 0] = Pr[B(m) = 1] = 1/2$. For example,

any function $B_i(m)$ = "i-th bit of m" is a one-bit information function. But there are many others, for example, $B(m)$ could be defined as an xor of all bits of m, or a majority of all bits of m, etc.

Again, propose a formal definition of an encryption scheme which is secure in the sense of infeasibility of deciding significantly better than at random any one-bit information function on m, given only an encryption of m, for a random m.

Then either prove that every indistinguishable encryption scheme is secure in this new sense, or give a counterexample.

2.4 Conclusion

Which of the three security properties seems strongest? Which one seems weaker? Which one seems weakest?

3 Computations in $\mathbb{Z}_p^*$: Generating instances of a discrete-log-based OWF collection.

We'll construct a PPT algorithm which on input (p, q), where p is prime and q is a prime factor of $p-1$ whose length is polynomially related to the length of p (for simplicity of an argument, consider for example only q's s.t. $|q| \geq |p|/2$), outputs an element g in $\mathbb{Z}_p^*$ whose order is at least q, with a significant probability.

Recall than an order $ord_p(x)$ of an element x of $\mathbb{Z}_p^*$ is defined as the smallest integer i s.t. $x^i = 1 \bmod p$.

3.1

Recall the Euler's theorem that $x^{p-1} = 1 \bmod p$ for all x. Show that for every x, $ord_p(x)$ divides $p-1$.

3.2

Prove that if $z^{(p-1)/q} \neq 1 \bmod p$ then $ord_p(z)$ is at least q. (Consider all prime factors $q_0, q_1, ..., q_e$ of $p-1$ where $q_0 = q$. Note that $p-1/q$ is a multiple of q_i for all $i \neq 0$.)

3.3

Recall that if p is prime then $\mathbb{Z}_p^*$ is a cyclic group and hence has a generator g. Therefore for every $z \in \mathbb{Z}_p^*$ there is a unique index $i_z \in \mathbb{Z}_{p-1}$ s.t. $g^{i_z} = z \bmod p$. Show that $ord_p(z) = r$ if and only if $i_z * ord_p(z) = 0 \bmod p-1$.

3.4

Show that for every r, there are at most r elements of $\mathbb{Z}_p^*$ whose order is r.

3.5

Show that there can be at most $|p|$ different prime factors of $p-1$.

3.6

Consider an algorithm A which picks a random element $z \in \mathbb{Z}_p^*$, and outputs z if $z^{(p-1)/q} \neq 1 \bmod p$ (and fails otherwise). By subsection 3.2, if this algorithm succeeds, it outputs an element of an order at least q.

Now use the results of subsections 3.4 and 3.5 to show that A has a significant probability of success.

3.7

A random k-bit number is prime with probability about $1/k$. Moreover, for a random $k/2$-bit prime q, the probability that $p = iq + 1$ for a random $k/2$-bit i is prime as well, is again about $1/k$. Show that this immediately implies a simple PPT algorithm to generate a pair of primes p, q s.t. $|p| = k$ and $|q| = k/2$ and q divides $p - 1$.

3.8 Conclusion

Since the discrete logarithm problem of finding x on input a random $y \in \mathbb{Z}_p^*$ s.t. $g^x = y \bmod p$, is believed hard if the order of g is divisible by a large prime q (e.g. $|q| = k/2$), the combined procedure of subsections 3.6 and 3.5 creates a PPT algorithm which generates (with significant probability) an instance of a one-way function collection based on the discrete logarithm problem: The instance of this OWF collection for a security parameter k is a function $f_{(g,p)}$ (for g, p as above) defined on $\mathbb{Z}_{p-1}$ as $f_{(g,p)}(x) = g^x \bmod p$.