CSL 759 – Cryptography and Network Security	Jan 10, 2014
Lecture 4	
Instructor: Shweta Agrawal	*Scribe: Amitabh Saraswati*

1 Introduction

1.1 Complexity Theoretic Approach

We make the weakest possible assumption and assume that a weak OWF exists since there is a low risk in making this assumption. Then, we transform it in a generic manner to build a strong OWF. Eg. We concatenated several instances of a weak OWF together to build a strong OWF in the last class.

1.2 Number Theoretic Approach

If we know a problem to be a hard problem, i.e, we start with the assumption of a strong OWF, we choose the domain such that we get a strong OWF. Eg. Discrete Log Problem
Candidates from Number Theory $f(p, q) = p * q$, where p and q are k-bit primes
Conjecture: p*q is hard to factor (but not always). We will see denotion of Weak One Way Function in next lecture.

2 Discrete Log Problem

2.1 Setup

Let G be a group of order p and let g be a generator of G. A group is a set of elements with the following four properties:

1. Closure
2. Associativity
3. Identity
4. Inverse

${Z_n}^* = \{ x|x$ belongs to Z_n and $gcd(x, n) = 1 \}$ and the order of this set is given by Euler's Phi Function, i.e., $phi(n)$ = number of elements co-prime to n.
If n = prime p, $phi(n) = p - 1$

Theorem 1 *Fermat's Little Theorem: If a belongs to ${Z_p}^*$, $a^{p-1} = 1 \ mod \ p$*

Proof. Lagrange's Theorem states that the order of any element divides the order of the group.
Now, consider an element a of order i. By Lagrange's Theorem, $i|p-1$. Also, $a^i = 1$ mod p. So, $a^{i(p-1)/i} = 1$ mod p. Hence, $a^{p-1} = 1$ mod p. qed

2.2 Function

For ${Z_p}^*$, there exists g of order $p-1$. Such a g is a generator of ${Z_p}^*$.

Consider the function $f(x) = g^x$ mod p.
Conjecture: If we choose p to be a random k bit prime and g as a random generator, $f(x)$ is hard to invert. Note that this is a direct conjecture of $f(x)$ being a strong OWF.

Given $y = g^x$ mod p, it is hard to recover x. But does this mean that x is completely hidden?
No, it turns out the LSB of x can be computed efficiently using "Quadratic Residues".