Advanced Cryptography — Retake Exam

Serge Vaudenay

2.9.2008

1 On Orthomorphisms

Definition 1. *Given a set $\mathcal{Z}$ of n elements,*

- *a* Latin square *is a $n \times n$ array of elements in $\mathcal{Z}$ such that each row and each column is a permutation of $\mathcal{Z}$;*
- *two Latin squares A and B are* orthogonal *if for each $(a,b) \in \mathcal{Z}^2$ there exist indices i and j such that $A_{i,j} = a$ and $B_{i,j} = b$.*

Given an (additively denoted) group G of order n,

- *a Cayley table is a $n \times n$ array such that the first row and the first column are permutations of G and for each i and j we have $A_{i,j} = A_{i,1} + A_{1,j}$;*
- *an orthomorphism is a permutation σ over G such that $x \mapsto \sigma(x) - x$ is also a permutation over G.*

We consider a group G of order n and we take $\mathcal{Z} = G$.

1. Show that a Cayley table is a Latin square.
2. Show that if σ is an orthomorphism and A is a Cayley table then the array B defined by $B_{i,j} = A_{i,1} + \sigma(A_{1,j})$ is a Latin square orthogonal to A.
3. Show that if A and B are two orthogonal Latin squares then there exists a unique function f over $\mathcal{Z}^2$ such that $f(A_{i,1}, A_{1,j}) = (A_{i,j}, B_{i,j})$. Show that it is a multipermutation.
4. Show that if $G = (\{0,1\}^n)^2$ then $\sigma(a,b) = (b, a \oplus b)$ is an orthomorphism.

2 The Rabin Cryptosystem

Given $N = p \times q$ for two different large prime numbers p and q, we define $\mathsf{Enc}_N(x) = x^2 \bmod N$ over the $\mathbf{Z}_N$ set.

1. Is $\mathbf{Z}_N$ a permutation?
2. Assume that $p \bmod 4 = q \bmod 4 = 3$. Given y, give a formula to compute all x such that $\mathsf{Enc}_N(x) = y$.
3. Show that given an oracle such that when queried with a random $y \in \mathbf{Z}_N$ it answers x such that $\mathsf{Enc}_N(x) = y$ with probability ρ we can mount an algorithm to factor N with complexity $O(1/\rho)$.
4. Let $R : \{0,1\}^\ell \longrightarrow \mathbf{Z}_N$ be an injective function, easy to evaluate and to invert, such that $2^\ell \ll N$. We define $\mathsf{Enc}'_N(R(x)) = x^2 \bmod N$ from $\{0,1\}^\ell$ to $\mathbf{Z}_N$. Show that we can invert Enc'_N with high probability when we know p and q. Does the algorithm of the previous question work?
5. Is Enc'_N semantically secure? Propose a construction.