E0 235 Cryptography : Aug. - Dec. 2006
Implementation and Exeperimentation : 25 marks

The Stream cipher exercise given in class carries 15 Marks and the following exercise (assigned as indicated) carries 10 Marks

1. Implement the three schemes for hash functions ([MOV] pp.341) based on the three block ciphers DES, IDEA and AES (Rijndael)

2. Consider integers in the range $(i-1)*2^{256}+1-i*2^{256}, i=2,\ldots$. Let $K=1000$. Generate K *Sophie Germain* primes, p,q of the form $p=2*q+1$, with $q \in S$. Determine the number of primitive roots $g, g \in \{2,\ldots,100\}$.

3. Consider the finite field F_q with $q=2^n$. Fix $n=512$. Determine a certain number K (say, $K=100$), of *sparse* irreducible polynomials f of degree n over F_2, with sparsity factors $m=3,5$. Sparsity factor is the number of nonzero terms in the polynomial f, other than the terms x^n and $x^0=1$. Now consider another class of *almost sparse* polynomials f defined by

$$f(x) = g_t(x)x^{M_{t-1}} + \ldots + g_2(x)x^{M_1} + g_1(x),$$

where $g_1, g_2, \ldots, g_t$ are all polynomials of *low* degree (say 3). Determine such irreducible polynomials of degree n over F_2. Your algorithm must use t as a parameter and obtain the results for values of $1 \leq t \leq 5$.

4. The following assignments are to obtain computational results on properties of divisors of smooth integers s, in the interval $I=2^M \leq s \leq 2^M+2^N$, for a smoothness bound $B=2^K$. Values to be fixed are: $M=120,240, N=24, K=32$. The properties to be studied are: (i) the total number n_b of distinct prime divisors $q<B$ of s classified according to the sizes of q in bits b. Your answer will be a one row table, of n_b vs b. (ii) the total number n_e of distinct prime divisors $q<b$ of s classified according to the exponents e and the sizes of q in bits b. Your answer will be a matrix table, of n_e w.r.t e and b.

5. The following assignments are to obtain computational results on properties of divisors of smooth integers $s=p-1, p$ *prime*, in the interval $I=2^M \leq s \leq 2^M+2^N$, for a smoothness bound $B=2^K$. Values to be fixed are: $M=64, N=24, K=32$. The properties to be studied are: (i) the total number n_b of distinct prime divisors $q<B$ of s classified according to the sizes of q in bits b. Your answer will be a one row table, of n_b vs b. (ii) the total number n_e of distinct prime divisors $q<b$ of s classified according to the exponents e and the sizes of q in bits b. Your answer will be a matrix table, of n_e w.r.t e and b.

6. The following assignments are to obtain computational results on properties of divisors of smooth integers $s=p+1, p$ *prime*, in the interval

$I = 2^M \leq s \leq 2^M + 2^N$, for a smoothness bound $B = 2^K$. Values to be fixed are: $M = 64, N = 24, K = 32$. The properties to be studied are: (i) the total number n_b of distinct prime divisors $q < B$ of s classified according to the sizes of q in bits b. Your answer will be a one row table, of n_b vs b. (ii) the total number n_e of distinct prime divisors $q < b$ of s classified according to the exponents e and the sizes of q in bits b. Your answer will be a matrix table, of n_e w.r.t e and b.

7. Implement the MPQS algorithm. Provide timing details for factoring *compositors of 64 bits* and *tricomposites of 96 bits*. Provide timing details for factoring 120, 240 bit *arbitrary* integers.

Stream Cipher assignment

Choose and implement any stream cipher. Collect good amount of statistical data for it (using a tool from *Informatics Lab*) after encrypting various kinds of data (plain-text, image, audio, etc.,.).