

**LAHORE UNIVERSITY OF MANAGEMENT SCIENCES
CENTRE FOR ADVANCED STUDIES IN MATHEMATICS**

**WORKSHOP ON COMPUTATIONAL
NUMBER THEORY & CRYPTOGRAPHY
(April 16-17, 2005)**

16th April, 2005 (Saturday)

| Sr. | Time | Topics and Speaker |
|------------|-------------|---|
| 1. | 8:40-9:10 | Registration |
| 2. | 9:15-10:45 | <i>Introduction to computational number theory and cryptography.</i> Arif Zaman Lahore University of Management Sciences, Lahore. |
| 3. | 10:45-11:30 | <i>Break</i> |
| 4. | 11:30-1:00 | <i>Modular arithmetic, computing in Z_n, repeated squaring and the discrete log problem, solving linear equations in Z_n, theorems of Euler and Fermat.</i> Sarmad Abbasi National University of Computer & Emerging Sciences, Lahore. |
| 5. | 1:00-2:30 | <i>Break</i> |
| 6. | 2:30-4:00 | <i>Basic public key cryptography: RSA, Diffie-Hellman, ElGamal and other cryptosystems; Cryptographic protocols and attacks.</i> Sarmad Abbasi National University of Computer & Emerging Sciences, Lahore. |
| 7. | 4:00-5:00 | <i>Break</i> |
| 8. | 5:00-6:30 | Problem Solving Session with TA's |
| 9. | 7:30-8:30 | Workshop Dinner at EDC. |

17th April, 2005 (Sunday)

| | | |
|-----|-------------|--|
| 10. | 9:15-10:45 | <i>Primality testing: Quadratic reciprocity, pseudo-primes, Euler pseudo-primes, strong pseudo-primes. Generating random prime numbers. Deterministic primality testing.</i> Arif Zaman Lahore University of Management Sciences, Lahore. |
| 11. | 10:45-11:30 | <i>Break</i> |
| 12. | 11:30-1:00 | <i>Integer factoring and solving the discrete log problem.</i> Sarmad Abbasi National University of Computer & Emerging Sciences, Lahore. |
| 13. | 1:00-2:30 | <i>Break</i> |
| 14. | 2:30-4:00 | <i>Galois fields, elliptic curves and elliptic curve cryptography.</i> Arif Zaman Lahore University of Management Sciences, Lahore. |
| 15. | 4:00-5:00 | <i>Break</i> |
| 16. | 5:00-6:30 | Problem Solving Session with TA's |