COSC/MATH 314 Spring 2017

You can bring to the exam 2 pages hand-written on both sides with whatever you want.

List of topics for final exam

- Primes, Euclidean Alg., Extended Euclidean Alg.
- Modular arithmetic, Chinese Remainder Th.
- Modular exponentiation, Fermat's Little Theorem, Euler's Theorem.
- Primitive roots modulo p.
- Square roots modulo n (when n is prime or product of two prime numbers).
- Finite fields; operations in $GF[2^n]$.
- RSA, basic algorithms and analysis, attacks, implementation.
- Primality testing, Miller-Rabin probabilistic test.
- The general concept of a public-key cryptosystem.
- The discrete log problem.
- Diffie-Hellman key exchange protocol.
- El Gamal public-key cryptosystem.
- Semantic security; non-malleability; OAEP.
- Hash functions; requierements, Merkle-Damgard scheme, birthday paradox.
- Message authentication codes; HMAC, CBC-MAC.
- Digital signatures; general concept, El Gamal digital signature, DSA, hash+sign issues.
- Station-to-station protocol, ssh identification protocol, Schnorr identification protocol, zero-knowledge, Fiat-Shamir protocol.