Final Exam   WED 5/5

exam: $1^{00} - 3^{00}$ PM   upload work by 3^{30} PM
PDF

format
- like for midterm exams
- show-your-work problems ~ 4
- short answer problems ~ 16
  no "real" work needed

practice
- review HW
- practice problems + solutions

tools
- calculators allowed   but: show work
- notes allowed   but: watch time

Questions ?

not on the exam   historical ciphers, credit cards, CSS

- review of number theory
  congruences, modular inverses (Euclid!),
  phi function, little Fermat + Euler,
  numbers in different bases
- binary exponentiation
- one-time pad
- stream ciphers + PRGs
  LCG
  LFSR, period
- Chinese remainder theorem
  solving quadratic equations
  number of solutions
  quadratic residues
- Blum-Blum-Shub
- primes + primality testing
  Fermat + Miller-Rabin, liars
  PNT

BLOCK CIPHERS

- DES , 3DES
- AES

  ⟹ finite fields : multiply + invert
- block cipher modes

  ECB , CBC

PUBLIC KEY CRYPTO

- RSA public : (N, e) private : d
- Diffie-Hellman key exchange

  ⟹ multiplicative order ,
  primitive roots (numbers of , list all)
- ElGamal public : (p, g, h) private : x

  $h = g^{x} \pmod{p}$

HASH FUNCTIONS

- Merkle-Damgard construction
- application: human passwords
- application : digital signatures
- birthday paradox

- elliptic curves