Midterm #2 — WED 4/7

exam: 1:25 – 2:15 PM upload work by 2:45 PM
PDF

format
- like for first exam
- show-your-work problems ~ 3
- short answer problems ~ 10
  - no "real" work needed

practice
- review HW
- practice problems + solutions

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

Questions?

- previously: background, stream ciphers + PRGs, primality testing
- now: block ciphers, public key cryptography

- DES, 3DES
- AES
  => finite fields: multiply + invert
- block cipher modes
  ECB, CBC

- RSA public: (N, e) private: d
- Diffie-Hellman key exchange
  => multiplicative order, primitive roots (number of, list all)
- ElGamal public: (p, g, h) private: x

EG $GF(2^5)$ constructed via x^5+x^2+1

Invert x^4. 10000

$$x^5+x^2+1 \equiv x \cdot x^4 + x^2+1$$

$$x^4 = (x^2+1)(x^2+1) + 1$$

$$(x^5+x^2+1) \div x^4 = x$$
$$-x^5$$
$$x^2+1$$

$$\Rightarrow 1 = x^4 + (x^2+1)(x^2+1)$$

$$= (1+(x^2+1)x)\,x^4 + (x^2+1)(x^5+x^2+1)$$

$\equiv 0$

$$x^4 \div (x^2+1) = x^2+1$$
$$-(x^4+x^2)$$
$$x^2$$
$$-(x^2+1)$$
$$1$$

$$\Rightarrow (x^4)^{-1} \equiv 1+(x^2+1)x = x^3+x+1$$

in bits: 01011

EG ElGamal $g^x \pmod p$

public key: (p, g, h) private key: x

encrypt: $c = (c_1, c_2) = (g^y, h^y m) \pmod p$

decrypt: $m = g^{-xy} c_2 \pmod p$

$g^{-xy} = c_1^{-x}$