Midterm #2

MATH 481/581 — Cryptography
Wednesday, Apr 5

Please print your name:

No notes, calculators or tools of any kind are permitted. There are 36 points in total. You need to show work to receive full credit.

Good luck!

Problem 1. (3+3 points) Bob's public ElGamal key is $(p, g, h) = (19, 10, 6)$.

(a) Encrypt the message $m = 5$ ("randomly" choose $y = 2$) and send it to Bob.

(b) Break the cryptosystem and determine Bob's secret key.

Problem 2. (4 points) You are Eve. Alice and Bob select $p = 41$ and $g = 7$ for a Diffie–Hellman key exchange. Alice sends 15 to Bob, and Bob sends 38 to Alice. What is their shared secret?

Armin Straub
straub@southalabama.edu

Problem 3. (3+3 points) Bob's public RSA key is $N = 33$, $e = 13$.

(a) Encrypt the message $m = 5$ and send it to Bob.

(b) Determine Bob's secret private key d.

Problem 4. (1+3 points) Consider the finite field $\mathrm{GF}(2^3)$ constructed using $x^3 + x + 1$.

(a) Multiply $x^2 + 1$ and x in $\mathrm{GF}(2^3)$.

(b) Determine the inverse of $x^2 + x$ in $\mathrm{GF}(2^3)$.

Armin Straub
straub@southalabama.edu

Problem 5. (16 points) Fill in the blanks.

(a) If Bob's public RSA key is (N, e) and Bob's secret key is d, then how does Bob decrypt the ciphertext c?

The plaintext is $m =$ ____.

(b) For his public RSA key, which of p, q and e must Bob choose randomly? ____

(c) For his public ElGamal key, which of p, g and x must Bob choose randomly? ____

(d) Despite its flaws, in which scenario is it fine to use the Fermat primality test?

____

(e) DES has a block size of ____ bits, a key size of ____ bits and consists of ____ rounds.

(f) To store an S-box in DES as a lookup table, we need ____ bytes.

(g) Suppose we are using 3DES with key $k = (k_1, k_2, k_3)$, where each k_i is an independent DES key.

Then m is encrypted to $c =$ ____. The effective key size is ____ bits.

(h) AES-128 has a block size of ____ bits, a key size of ____ bits and consists of ____ rounds.

(i) The four layers of AES are ____.

(j) For his public ElGamal key, Bob selected $p = 101$. He has ____ choices for g.

(k) For his public RSA key, Bob selected $N = 77$. The smallest choice for e with $e \geqslant 2$ is ____.

(l) The primitive roots modulo 5 are ____.

(extra scratch paper)