Preparing for Midterm #2

MATH 481/581 — Cryptography
Midterm: Friday, Mar 29, 2024

Please print your name:

Bonus challenge. Let me know about any typos you spot in the posted solutions (or lecture sketches). Any typo, that is not yet fixed by the time you send it to me, is worth a bonus point.

Problem 1.

(a) If you can only do a single modular computation, how would you check whether a huge randomly selected number N is prime or not?

(b) Which flaw of the Fermat primality test renders it unsuitable as a general primality test? How can this flaw be fixed?

(c) Despite the flaw in the previous item, in which scenario is it fine to use the Fermat primality test regardless?

(d) We want to use the Miller–Rabin primality test to decide whether $N = 377$ is prime. Each time, we randomly choose a base a (and only do a single iteration of Miller–Rabin) and compute the following:

- $a = 12$: $12^{47} \equiv 220$, $12^{94} \equiv 144$, $12^{188} \equiv 1$, $12^{376} \equiv 1 \pmod{377}$
- $a = 70$: $70^{47} \equiv 307$, $70^{94} \equiv 376$, $70^{188} \equiv 1$, $70^{376} \equiv 1 \pmod{377}$
- $a = 80$: $80^{47} \equiv 332$, $80^{94} \equiv 140$, $80^{188} \equiv 373$, $80^{376} \equiv 16 \pmod{377}$
- $a = 233$: $233^{47} \equiv 233$, $233^{94} \equiv 1$, $233^{188} \equiv 1$, $233^{376} \equiv 1 \pmod{377}$

In each case, what do we conclude? (Also point out which calculations were unnecessary.) Which of the a are strong liars? Which are Fermat liars?

(e) Repeat the previous problem for $N = 247$ and the following computations:

- $a = 12$: $12^{123} \equiv 246$, $12^{246} \equiv 1 \pmod{247}$
- $a = 17$: $17^{123} \equiv 64$, $17^{246} \equiv 144 \pmod{247}$
- $a = 27$: $27^{123} \equiv 170$, $27^{246} \equiv 1 \pmod{247}$
- $a = 68$: $68^{123} \equiv 1$, $68^{246} \equiv 1 \pmod{247}$

Problem 2. Bob's public RSA key is $N = 65$, $e = 5$.

(a) Encrypt the message $m = 10$ and send it to Bob.

Armin Straub
straub@southalabama.edu

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

(c) You intercept the message $c = 2$ from Alice to Bob. Decrypt it using the secret key.

Problem 3. Bob's public ElGamal key is $(p, g, h) = (61, 10, 21)$.

(a) Encrypt the message $m = 11$ ("randomly" choose $y = 17$) and send it to Bob.

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

(c) Use the secret key to decrypt $c = (13, 7)$.

Problem 4.

(a) For his public RSA key, Bob has selected $N = 91$. What is the smallest choice for e with $e \geqslant 2$?

(b) How many primitive roots are there modulo 13? Determine all of them.

(c) Find x such that $9 \equiv 7^x \pmod{13}$.

(d) For his public ElGamal key, Bob has selected $p = 61$. How many possible choices does he have for g?

(e) Alice and Bob select $p = 61$ and $g = 55$ for a Diffie–Hellman key exchange. Alice sends 32 to Bob, and Bob sends 54 to Alice. What is their shared secret?

(f) Determine the multiplicative orders of $2, 4, 8, 16$ modulo 61. Are any of these primitive roots? How many primitive roots are there in total?

(g) Spell out the computational Diffie–Hellman problem as well as the decisional Diffie–Hellman problem. Which of these is more difficult?

(h) For his public RSA key, Bob needs to select p, q and e. Which of these must be chosen randomly?

(i) For his public ElGamal key, Bob needs to select p, g and x. Which of these must be chosen randomly?

(j) When using vanilla RSA, why must we never directly encrypt messages that can be predicted (like "yes", "no", "maybe"; or a social security number)?

Armin Straub
straub@southalabama.edu

Problem 5. Consider the finite field $\mathrm{GF}(2^4)$ constructed using x^4+x+1.

(a) Add and multiply x^2+1 and x^2+x+1 in $\mathrm{GF}(2^4)$.

(b) What is the inverse of x^2+x+1 in $\mathrm{GF}(2^4)$?

(c) What is the inverse of x^3+x in $\mathrm{GF}(2^4)$?

Problem 6.

(a) The design of a block cipher is almost an art, but there are two guiding principles due to Claude Shannon, the father of information theory.

- What are these two principles? Briefly explain what they refer to.
- Which of these are the classical ciphers lacking?

(b) In a Feistel cipher, how does the encryption in one round look like?

Can any function be used in this construction?

How does decryption work?

Problem 7.

(a) What is the block size of DES? What is the key size? How many rounds?

(b) What does each S-box do?

To store an S-box in DES as a lookup table, how many bytes are needed?

(c) How many bits are the round keys? How are they obtained?

(d) How does 3DES encryption work? What is the key?

What is the effective key size and why is it different?

(e) Why is there no 2DES?

(f) To (naively) brute-force DES, how much data must we encrypt?

Problem 8.

(a) What is the block size of AES? What is the key size? How many rounds?

(b) How is it possible that AES uses fewer rounds than DES?

(c) What are the four layers that each round consists of?

(d) Which layer makes AES highly nonlinear? Describe the crucial mathematical operation involved in this layer.

(e) To store the ByteSub layer of AES as a lookup table, how many bytes are needed?

Problem 9. Consider a block cipher with 5 bit block size and 5 bit key size such that

$$E_k(b_1b_2b_3b_4b_5) = (b_2b_5b_4b_3b_1) \oplus k.$$

(a) Encrypt $m = (010101010101010\ldots)_2$ using $k = (10001)_2$ and ECB mode.

(b) Encrypt $m = (010101010101010\ldots)_2$ using $k = (10001)_2$ and CBC mode ($\mathrm{IV} = (10011)_2$).