1 Preparing for Midterm 2

- These problems are taken from the lectures to help you prepare for our upcoming midterm exam. You can find solutions to all of these in the lecture sketches.
- I will also post additional practice problems before the end of the week.

Example 1. Fermat's little theorem can be stated in the slightly stronger form:

n is a prime $\iff$ [ ] for all $a \in \{1, 2, \ldots, n-1\}$

Fermat primality test

Input:

Output:

Algorithm:

a is called a **Fermat liar** if [ ].

On the other hand, a is called a **Fermat witness** if [ ].

Flaw. Describe a reason why the Fermat primality test is not used as a general test for primality.

Example 2. Suppose we want to determine whether $n = 221$ is a prime. Simulate the Fermat primality test for the choices $a = 38$ and $a = 24$.

Is one of these a Fermat liar or Fermat witness?

Example 3. What are **absolute pseudoprimes** (or Carmichael numbers)?

Example 4. How can you check whether a huge randomly selected number N is prime?

Miller–Rabin primality test

Input:

Output:

Algorithm:

Armin Straub
straub@southalabama.edu

Example 5. Suppose we want to determine whether $n = 221$ is a prime. Simulate the Miller–Rabin primality test for the choices $a = 24$, $a = 38$ and $a = 47$.

- Questions on block cipher design.
  - 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?
  - 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?
- Questions on DES.
  - What is the block size of DES? What is the key size? How many rounds?
  - What does each S-box do?
  - How many bits are the round keys? How are they obtained?
  - How does 3DES encryption work? What is the key?
    What is the effective key size and why is it different?
  - Why is there no 2DES?
  - To (naively) brute-force DES, how much data must we encrypt?
- Questions on AES.
  - What is the block size of AES? What is the key size? How many rounds?
  - How is it possible that AES uses less rounds than DES?
  - What are the four layers that each round consists of?
  - Which layer makes AES highly nonlinear? Describe the crucial mathematical operation involved in this layer.

Example 6. Why are the residues modulo 21 (or any other composite number) not a field?

To construct the finite field $\mathrm{GF}(p^n)$ of p^n elements, we can do the following:

-
- The elements of $\mathrm{GF}(p^n)$ are ______.

Example 7. The polynomial $x^2 + x + 1$ is irreducible modulo 2, so we can use it to construct the finite field $\mathrm{GF}(2^2)$ with 4 elements.

(a) List all 4 elements, and make an addition table. Then realize that this is just xor.

Armin Straub
straub@southalabama.edu

(b) Make a multiplication table.

(c) What is the inverse of $x+1$?

Example 8. The polynomial x^3+x+1 is irreducible modulo 2, so we can use it to construct the finite field $\mathrm{GF}(2^3)$ with 8 elements.

(a) List all 8 elements, and multiply all of them with $x+1$.

(b) What is the inverse of $x+1$?

Example 9.

(a) Apply the extended Euclidean algorithm to find the gcd of x^2+1 and x^4+x+1, and spell out Bezout's identity.

(b) Repeat the previous computation but always reduce all coefficients modulo 2.

(c) What is the inverse of x^2+1 in $\mathrm{GF}(2^4)$? Here, $\mathrm{GF}(2^4)$ is constructed using x^4+x+1.

Example 10. Find the inverse of x^2+1 in $\mathrm{GF}(2^8)$, constructed using $x^8+x^4+x^3+x+1$ (as in AES).

Example 11.

(a) Apply the extended Euclidean algorithm to find the gcd of x^3+1 and $x^8+x^4+x^3+x+1$, and spell out Bezout's identity.

(b) Repeat the previous computation but always reduce all coefficients modulo 2.

(c) What is the inverse of x^3+1 in $\mathrm{GF}(2^8)$, constructed using $x^8+x^4+x^3+x+1$?

(RSA encryption)

- Bob chooses .
-
- Public key:
  Secret private key:
- Alice encrypts .
- Bob decrypts .

Example 12. If $N=77$, what is the smallest (positive) choice for e in RSA?

Example 13. Bob's public RSA key is $N=55$, $e=7$.

(a) Encrypt the message $m=8$ and send it to Bob.

(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.

Example 14. Bob's public RSA key is $N=77$, $e=13$.

(a) Encrypt the message $m=2$ and send it to Bob.

(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.

Example 15. Is it a problem that $m=1$ is always encrypted to $c=1$? (Likewise for $m=0$.)

Example 16. RSA is so cool! Why do we even care about, say, AES anymore?

Example 17. When using RSA, why must we never directly encrypt messages that can be predicted (like a social security number)?

Example 18. Bob's public RSA key is $N=33$, $e=3$.

(a) Encrypt the message $m=4$ and send it to Bob.

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

(c) You intercept the message $c=31$ from Alice to Bob. Decrypt it using the secret key.

Theorem 19.

Determining the secret private key d in RSA is as difficult as __________.

- Whereas the security of RSA relies on the difficulty of factoring, the security of ElGamal relies on the difficulty of __________.

Example 20. Find x such that $4 \equiv 3^x \pmod{7}$.

Example 21. Check that $x=69$ solves $3 \equiv 2^x \pmod{101}$.

(ElGamal encryption)

- Bob chooses __________.
- Public key:
  Secret private key:
- To encrypt, Alice ...
- Bob decrypts __________.

Example 22. Bob chooses the prime $p = 31$, $g = 11$, and $x = 5$. What is his public key?

Example 23. Bob's public ElGamal key is $(p, g, h) = (31, 11, 6)$.

(a) Encrypt the message $m = 3$ ("randomly" choose $y = 4$) and send it to Bob.

(b) Recall that Bob's secret private key is $x = 5$. Use it to decrypt $c = (9, 13)$.

Example 24. Bob's public ElGamal key is $(p, g, h) = (41, 7, 20)$.

(a) Encrypt the message $m = 10$ ("randomly" choose $y = 15$) and send it to Bob.

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

(c) Use the secret key to decrypt $c = (15, 16)$.

Example 25. Bob's public ElGamal key is $(p, g, h) = (23, 10, 11)$.

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

(b) Encrypt the message $m = 5$ ("randomly" choose $y = 4$) and send it to Bob.

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

(d) Use the secret key to decrypt $c = (8, 7)$.

(e) Likewise, decrypt $c = (18, 19)$.

Example 26. If Bob selects $p = 23$, how many possible choices does he have for g? Which are these?

We indicated that the security of ElGamal depends on the difficulty of computing discrete logarithms. Here is a more precise statement.

Theorem 27. Decrypting c to m in ElGamal is exactly as difficult as [ ].

Describe this problem.

(Diffie–Hellman key exchange)

-
-
- As above, Alice and Bob now share the secret [ ].

Example 28. You are Eve. Alice and Bob select $p = 53$ and $g = 5$ for a Diffie–Hellman key exchange. Alice sends 43 to Bob, and Bob sends 20 to Alice. What is their shared secret?