Midterm #1

MATH 481/581 — Cryptography
Friday, Feb 16, 2024

Please print your name:

No notes, calculators or tools of any kind are permitted. There are 40 points in total. You need to show work to receive full credit.

Good luck!

Problem 1. (7+1 points) Eve intercepts the ciphertext $c = (111\ 111\ 000)_2$. She knows it was encrypted with a stream cipher using the linear congruential generator $x_{n+1} \equiv 5x_n + 1 \pmod{8}$ as PRG.

(a) Eve also knows that the plaintext begins with $m = (010\ 1\ldots)_2$. Break the cipher and determine the plaintext.

(b) Eve was able to crack the ciphertext because the PRG is lacking a property that is crucial for cryptography. Which property is that?

Problem 2. (4 points)

(a) Suppose N is composite. x is a Fermat liar modulo N if and only if ______.

(b) $7 \pmod{10}$ ☐ is a Fermat liar ☐ is not a Fermat liar because ______.

(scratch space: show your work for partial credit)

Armin Straub
straub@southalabama.edu

Problem 3. (6 points) Using the Chinese remainder theorem, determine all solutions to $x^2 \equiv 4 \pmod{55}$.

Problem 4. (5 points) Evaluate $40^{16011} \pmod{34}$. Show your work!

Problem 5. (2 points) Briefly outline the Fermat primality test.

Problem 6. (15 points) Fill in the blanks.

(a) $2^{-1} \pmod{29} \equiv$ ______.

(b) Modulo 33, there are ______ invertible residues, of which ______ are quadratic.

(c) Modulo 31, there are ______ invertible residues, of which ______ are quadratic.

(d) 22 in base 2 is ______.

(e) The residue 10 is invertible modulo n if and only if ______.

(f) We have $\phi(mn) = \phi(m)\phi(n)$ provided that ______.

(g) How many solutions does the congruence $x^2 \equiv 9 \pmod{105}$ have? ______

How many solutions does the congruence $x^2 \equiv 16 \pmod{105}$ have? ______

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

______

(i) The first 5 bits generated by the Blum-Blum-Shub PRG with $M = 133$ using the seed 5 are ______.

You may use that $16^2 \equiv 123$, $25^2 \equiv 93$, $36^2 \equiv 99$, $92^2 \equiv 85$, $93^2 \equiv 4$, $99^2 \equiv 92 \pmod{133}$.

(j) Using a one-time pad and key $k = (1100)_2$, the message $m = (1010)_2$ is encrypted to ______.

(k) While perfectly confidential, the one-time pad does not protect against ______.

(l) The LFSR $x_{n+15} \equiv x_{n+14} + x_n \pmod{2}$ must repeat after ______ terms.

(m) Recall that, in a stream cipher, we must never reuse the key stream.

Nevertheless, we can reuse the key if we use a ______.

(n) Up to x, there are roughly ______ many primes.

(o) The approximate proportion of primes among numbers up to 2^{1024} is ______. (Simplify!)

Armin Straub
straub@southalabama.edu

(extra scratch paper)