Midterm #1

MATH 481/581 — Cryptography
Friday, Feb 17, 2023

Please print your name:

No notes, calculators or tools of any kind are permitted. There are 37 points in total. You need to show work to receive full credit.

Good luck!

Problem 1. (6 points) Eve intercepts the ciphertext $c = (101\ 101\ 011)_2$. She knows it was encrypted with a stream cipher using the linear congruential generator $x_{n+1} \equiv 5x_n + 3 \pmod{8}$ as PRG.

Eve further knows that the plaintext begins with $m = (111\ 0\ldots)_2$. Break the cipher and determine the plaintext.

Problem 2. (5 points) Evaluate $40^{1613} \pmod{17}$. Show your work!

Armin Straub
straub@southalabama.edu

Problem 3. (6 points) Using the Chinese remainder theorem, determine all solutions to $x^2 \equiv 16 \pmod{55}$.

Problem 4. (4 points)

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

(b) $8 \pmod{21}$ ☐ is a Fermat liar ☐ is not a Fermat liar because ______.

(scratch space: show your work for partial credit)

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

Armin Straub
straub@southalabama.edu

Problem 6. (14 points) Fill in the blanks.

(a) The residue x is invertible modulo n if and only if ________.

(b) $3^{-1} \pmod{29} \equiv$ ________.

(c) Modulo 29, there are ________ invertible residues, of which ________ are quadratic.

(d) Modulo 55, there are ________ invertible residues, of which ________ are quadratic.

(e) 24 in base 2 is ________.

(f) How many solutions does the congruence $x^2 \equiv 1 \pmod{105}$ have? ________

How many solutions does the congruence $x^2 \equiv 9 \pmod{105}$ have? ________

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

____

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

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

(i) Using a one-time pad and key $k = (0011)_2$, the message $m = (1010)_2$ is encrypted to ________.

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

(k) The LFSR $x_{n+31} \equiv x_{n+28} + x_n \pmod{2}$ must repeat after ________ terms.

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

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

(m) In order for a PRG to be suitable for use in a stream cipher, the PRG must be ________.

(n) As part of the Miller–Rabin test, it is computed that $26^{147} \equiv 495$, $26^{294} \equiv 1 \pmod{589}$.

What do we conclude? ________

Armin Straub
straub@southalabama.edu

(extra scratch paper)