

Midterm #1

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 points) Using the Chinese remainder theorem, determine all solutions to $x^2 \equiv 9 \pmod{55}$.

Problem 2. (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 3. (2 points) Briefly outline the Fermat primality test.

Problem 4. (6 points) Evaluate $23^{1613} \pmod{17}$.

Show your work!

Problem 5. (6 points) Eve intercepts the ciphertext $c = (001\ 001\ 001)_2$. 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 $m = (011\ 1\dots)_2$. Break the cipher and determine the plaintext.

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

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

(b) Recall that, in a stream cipher, we must never reuse the key stream.
Nevertheless, we can reuse the key if we use a

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

(d) While perfectly confidential, the one-time pad does not protect against

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

(f) The first 5 bits generated by the Blum-Blum-Shub PRG with $M = 133$ using the seed 5 are
You may use that $16^2 \equiv 123$, $25^2 \equiv 93$, $36^2 \equiv 99$, $92^2 \equiv 85$, $93^2 \equiv 4$, $99^2 \equiv 92 \pmod{133}$.

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

(h) 30 in base 2 is

(i) The residue x is invertible modulo n if and only if

(j) $2^{-1} \pmod{13} \equiv$

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

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

(m) We have $\phi(ab) = \phi(a)\phi(b)$ provided that

(n) How many solutions does the congruence $x^2 \equiv 4 \pmod{231}$ have?

$231 = 3 \cdot 7 \cdot 11$

(o) How many solutions does the congruence $x^2 \equiv 36 \pmod{231}$ have?

(extra scratch paper)