

Midterm #1

Please print your name:

No notes, calculators or tools of any kind are permitted. There are 33 points in total. You need to show work to receive full credit.

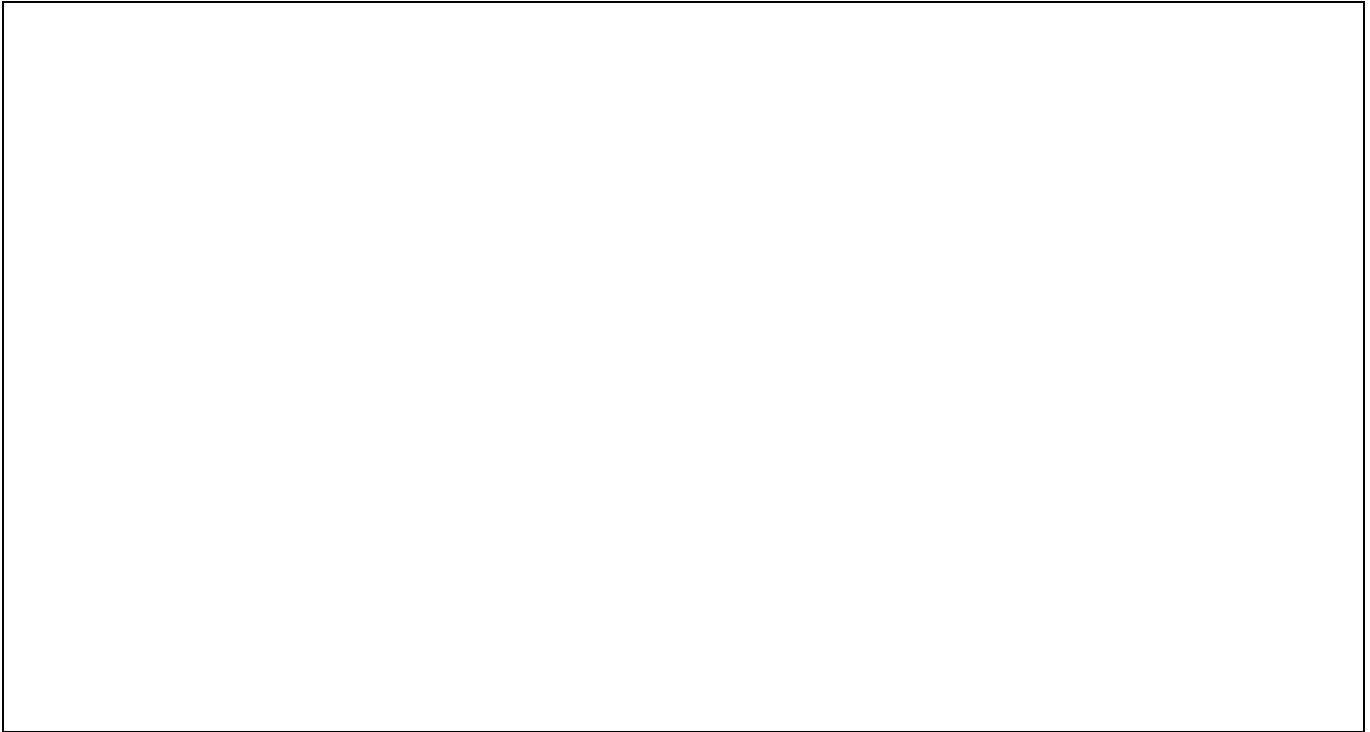
Good luck!

Problem 1. (7+1 points) Eve intercepts the ciphertext $c = (000\ 111\ 000)_2$. 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.

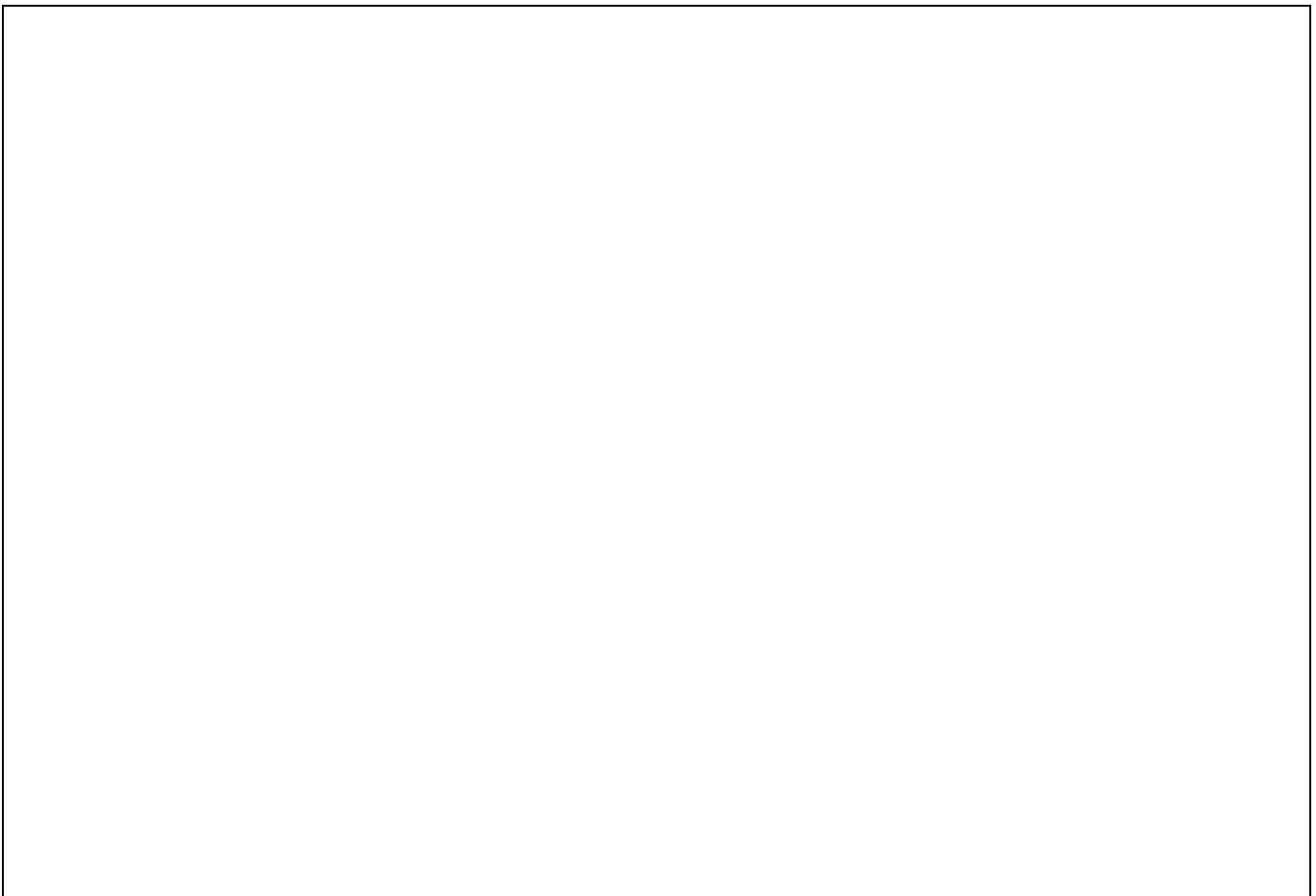
- (a) Eve also knows that the plaintext begins with $m = (011\ 1\dots)_2$. Break the cipher and determine the plaintext.
- (b) Eve was able to crack the ciphertext because the PRG is lacking a property that is crucial for cryptography. Which property is that?

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

Show your work!



Problem 3. (6 points) Using the Chinese remainder theorem, determine all solutions to $x^2 \equiv 1 \pmod{55}$.



Problem 4. (14 points) Fill in the blanks.

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

(b) $2^{-1} \pmod{31} \equiv$

(c) We have $\phi(mn) = \phi(m)\phi(n)$ provided that

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

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

(f) 11 in base 2 is

(g) A residue x modulo 221 is a Fermat liar if and only if

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

(i) The first three bits generated by the Blum-Blum-Shub PRG with $M = 77$ using the seed 37 are
You may use that, modulo 77, $37^2 \equiv 60$, $38^2 \equiv 58$, $39^2 \equiv 58$, $58^2 \equiv 53$, $59^2 \equiv 16$, $60^2 \equiv 58$.

(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 $x_{n+31} \equiv x_{n+28} + x_n \pmod{2}$ 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.

(extra scratch paper)