Midterm #1

MATH 481/581 — Cryptography
Wednesday, Feb 22

Please print your name:

No notes, calculators or tools of any kind are permitted. There are 32 points in total. You need to show work to receive full credit.

Good luck!

Problem 1. (8 points) Eve intercepts the ciphertext $c = (1101\ 0100\ 11)_2$. She knows it was encrypted with a stream cipher using a LFSR with $x_{n+3} \equiv x_{n+1} + x_n \pmod 2$ as PRG.

(a) Eve also knows that the plaintext begins with $m = (0001\ ...)_2$. Help her crack the ciphertext!

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

Armin Straub
straub@southalabama.edu

Problem 2. (5 points) Evaluate $383^{192} \pmod{38}$. [Simplify before binary exponentiation!]

Problem 3. (6 points)

(a) Using the Chinese remainder theorem, solve $x \equiv 6 \pmod{7}$, $x \equiv 1 \pmod{11}$. (Steps needed for full credit.)

(b) Using your answer from the first part, determine all solutions to $x^2 \equiv 1 \pmod{77}$.

Armin Straub
straub@southalabama.edu

Problem 4. (13 points) Fill in the blanks.

(a) Modulo 37, there are [ ] invertible residues, of which [ ] are quadratic.

(b) Modulo 77, there are [ ] invertible residues, of which [ ] are quadratic.

(c) The residue x is invertible modulo n if and only if [ ].

(d) $5^{-1} \pmod{11} \equiv$ [ ].

(e) If $n = p^2 q$, for distinct primes p, q, then $\phi(n) =$ [ ].

(f) 14 in base 2 is [ ].

(g) The multiplicative order of $2 \pmod{15}$ is [ ].

(h) The multiplicative order of x modulo n divides [ ].

(i) If $x \pmod{n}$ has multiplicative order k, then x^2 has multiplicative order [ ].

(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 $x_{n+7} \equiv x_{n+3} + x_n \pmod{2}$ 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 [ ].

(extra scratch paper)