Quiz #1

MATH 481/581 — Cryptography
Wednesday, Feb 19

Please print your name:

Problem 1. Fill in the blanks.

(a) $2^{-1} \pmod{31} \equiv$ ☐.

(b) We have $\phi(mn) = \phi(m)\phi(n)$ provided that ☐.

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

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

(e) 11 in base 2 is ☐.

(f) A residue x modulo 221 is a Fermat liar if and only if ☐.

(g) How many solutions does the congruence $x^2 \equiv 9 \pmod{77}$ have? ☐

(h) How many solutions does the congruence $x^2 \equiv 49 \pmod{77}$ have? ☐

(i) The first 3 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 $x_{n+15} \equiv x_{n+11} + x_n \pmod{2}$ 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 ☐.

Armin Straub
straub@southalabama.edu