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 ☐.

Solution.

(a) $2^{-1} \pmod{31} \equiv 16$.

Armin Straub
straub@southalabama.edu

(b) We have $\phi(mn) = \phi(m)\phi(n)$ provided that $\gcd(m,n) = 1$.

(c) Modulo 33, there are $\phi(33) = \phi(3)\phi(11) = 20$ invertible residues, of which $\frac{1}{4}\phi(33) = 5$ are quadratic.

(d) Modulo the prime 31, there are $\phi(31) = 30$ invertible residues, of which $\frac{1}{2}\phi(31) = 15$ are quadratic.

(e) 11 in base 2 is $(1011)_2$.

Comment. 11 was a bit ambiguous... $(11)_2$ in base 10 is 3.

(f) A residue x modulo 221 is a Fermat liar if and only if $x^{220} \equiv 1 \pmod{221}$.

(g) By the CRT, since $77 = 7 \cdot 11$, the congruence has $2 \cdot 2 = 4$ solutions.

(h) This congruence only has $1 \cdot 2 = 2$ solutions. (Note that $x^2 \equiv 49 \pmod 7$ only has one solution; namely, $x \equiv 0$.)

(i) The first three bits generated by the Blum-Blum-Shub PRG with $M = 77$ using the seed 37 are $0, 0, 1$ (obtained from $60, 58, 53$).

(j) Using a one-time pad and key $k = (1100)_2$, the message $m = (1010)_2$ is encrypted to $(0110)_2$.

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

(l) The LFSR $x_{n+15} \equiv x_{n+11} + x_n \pmod 2$ must repeat after $2^{15} - 1$ terms.

(m) We can reuse the key if we use a nonce.