Midterm #1

MATH 481/581 — Cryptography
Wednesday, Feb 20

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 $m = (011\ 1...)_2$. 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?

Solution.

(a) Since $c = m \oplus \text{PRG}$, we learn that the initial piece of the keystream is $\text{PRG} = c \oplus m = (000\ 111\ 000)_2 \oplus (011\ 1...)_2 = (011\ 0...)_2$.

Since each x_n has 3 bits, we learn that $x_1 = (011)_2 = 3$. Using $x_{n+1} \equiv 5x_n + 1 \pmod 8$, we find $x_2 = 0$, $x_3 = 1$, ... In other words, $\text{PRG} = 3, 0, 1, ... = (011\ 000\ 001\ ...)_2$.

Hence, Eve can decrypt the ciphertext and obtain $m = c \oplus \text{PRG} = (000\ 111\ 000)_2 \oplus (011\ 000\ 001)_2 = (011\ 111\ 001)_2$.

(b) Unpredictability. □

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

Solution. First, $40^{1613} \equiv 6^{1613} \pmod{17}$. Since $1613 \equiv 13 \pmod{\phi(17)}$, we have $6^{1613} \equiv 6^{13} \pmod{17}$.

Using binary exponentiation, we find $6^2 \equiv 2 \pmod{17}$, $6^4 \equiv 2^2 = 4 \pmod{17}$, $6^8 \equiv 4^2 \equiv -1 \pmod{17}$.

In conclusion, $40^{1613} \equiv 6^{13} = 6^8 \cdot 6^4 \cdot 6 \equiv -1 \cdot 4 \cdot 6 \equiv 10 \pmod{17}$. □

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

Solution. By the CRT:

$$\begin{aligned} & x^2 \equiv 1 \pmod{55} \\ \iff\ & x^2 \equiv 1 \pmod 5 \text{ and } x^2 \equiv 1 \pmod{11} \\ \iff\ & x \equiv \pm 1 \pmod 5 \text{ and } x \equiv \pm 1 \pmod{11} \end{aligned}$$

Hence, there are four solutions ± 1, $\pm a$ modulo 55. To find one of the nontrivial ones, we solve the congruences $x \equiv 1 \pmod 5$, $x \equiv -1 \pmod{11}$:

$$x \equiv 1 \cdot 11 \cdot \underbrace{11^{-1}_{\bmod 5}}_{1} - 1 \cdot 5 \cdot \underbrace{5^{-1}_{\bmod 11}}_{-2} \equiv 11 + 10 = 21 \pmod{55}$$

Hence, we conclude that $x^2 \equiv 1 \pmod{55}$ has the four solutions $\pm 1, \pm 21 \pmod{55}$. □

Armin Straub
straub@southalabama.edu

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

(a) The residue x is invertible modulo n if and only if $\boxed{}$.

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

(c) We have $\phi(mn) = \phi(m)\phi(n)$ provided that $\boxed{}$.

(d) Modulo 33, there are $\boxed{}$ invertible residues, of which $\boxed{}$ are quadratic.

(e) Modulo 31, there are $\boxed{}$ invertible residues, of which $\boxed{}$ are quadratic.

(f) 11 in base 2 is $\boxed{}$.

(g) A residue x modulo 221 is a Fermat liar if and only if $\boxed{}$.

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

$\boxed{}$

(i) The first three bits generated by the Blum-Blum-Shub PRG with $M = 77$ using the seed 37 are $\boxed{}$.

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 $\boxed{}$.

(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.

Solution.

(a) The residue x is invertible modulo n if and only if $\gcd(x,n) = 1$.

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

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

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

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

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

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

(h) Despite its flaws, it is fine to use the Fermat primality test for large random numbers.

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

(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 $x_{n+31} \equiv x_{n+28} + x_n \pmod 2$ must repeat after $2^{31} - 1$ terms.

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

(n) Up to x, there are roughly $x/\ln(x)$ many primes. □

(extra scratch paper)