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?

Solution.

(a) Since $c = m \oplus \text{PRG}$, we learn that the initial piece of the keystream is $\text{PRG} = m \oplus c = (0001\ ...)_2 \oplus (1101\ ...)_2 = (1100\ ...)_2$. Each x_n is 1 bit, and we have $x_1 = 1$, $x_2 = 1$, $x_3 = 0$.

Because the PRG is predictable, we can now recreate the entire keystream! Using $x_{n+3} \equiv x_{n+1} + x_n \pmod 2$, we find $x_4 \equiv x_2 + x_1 \equiv 0$ (which matches what we knew), $x_5 \equiv x_3 + x_2 \equiv 1$, ... Continuing, we find $\text{PRG} = (1100\ 1011\ 10...)_2$.

Hence, Eve can decrypt the ciphertext and obtain $m = c \oplus \text{PRG} = (1101\ 0100\ 11)_2 \oplus (1100\ 1011\ 10)_2 = (0001\ 1111\ 01)_2$.

(b) Unpredictability. □

Armin Straub
straub@southalabama.edu

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

Solution. Obviously, $383^{192} \equiv 3^{192} \pmod{38}$. We note that $\gcd(3, 38) = 1$, so that we may apply Euler's theorem.

Since $\phi(38) = \phi(2 \cdot 19) = 18$ and $192 \equiv 12 \pmod{18}$, we conclude that $3^{192} \equiv 3^{12} \pmod{38}$.

Using binary exponentiation, $3^2 = 9$, $3^4 = 9^2 \equiv 5$, $3^8 \equiv 25 \pmod{38}$. Hence, $3^{12} = 3^4 \cdot 3^8 \equiv 5 \cdot 25 \equiv 11 \pmod{38}$.

In summary, $383^{192} \equiv 11 \pmod{38}$.

□

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 $x^2 \equiv 1 \pmod{77}$.

Solution.

(a) $x \equiv 6 \cdot 11 \cdot \underbrace{11^{-1}_{\bmod 7}}_{2} + 1 \cdot 7 \cdot \underbrace{7^{-1}_{\bmod 11}}_{-3} = 132 - 21 \equiv 34 \pmod{77}$

(b) By the CRT:

$$\begin{aligned} & x^2 \equiv 1 \pmod{77} \\ \iff\ & x^2 \equiv 1 \pmod{7} \text{ and } x^2 \equiv 1 \pmod{11} \\ \iff\ & x \equiv \pm 1 \pmod{7} \text{ and } x \equiv \pm 1 \pmod{11} \end{aligned}$$

By the first part, $x \equiv -1 \pmod{7}$, $x \equiv 1 \pmod{11}$ has the solution $x \equiv 34 \pmod{77}$.

Hence, we conclude that $x^2 \equiv 1 \pmod{77}$ has the four solutions $\pm 1, \pm 34 \pmod{77}$.

□

Armin Straub
straub@southalabama.edu

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

(a) Modulo 37, there are $\boxed{}$ invertible residues, of which $\boxed{}$ are quadratic.

(b) Modulo 77, there are $\boxed{}$ invertible residues, of which $\boxed{}$ are quadratic.

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

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

(e) If $n = p^2 q$, for distinct primes p, q, then $\phi(n) = \boxed{}$.

(f) 14 in base 2 is $\boxed{}$.

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

(h) The multiplicative order of x modulo n divides $\boxed{}$.

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

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

Solution.

(a) Modulo 37, there are $\phi(37) = 36$ invertible residues, of which $\frac{1}{2}\phi(37) = 18$ are quadratic.

(b) Modulo 77, there are $\phi(77) = 60$ invertible residues, of which $\frac{1}{4}\phi(77) = 15$ are quadratic.

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

(d) $5^{-1} \pmod{11} \equiv -2$.

(e) If $n = p^2 q$, for distinct primes p, q, then $\phi(n) = n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = p(p-1)(q-1)$.

(f) 14 in base 2 is $(1110)_2$.

(g) The multiplicative order of $2 \pmod{15}$ is 4.

(h) The multiplicative order of x modulo n divides $\phi(n)$.

(i) If $x \pmod n$ has multiplicative order k, then x^2 has multiplicative order $k/\gcd(k, 2)$.

(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 $x_{n+7} \equiv x_{n+3} + x_n \pmod 2$ must repeat after $2^7 - 1 = 127$ terms.

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

(extra scratch paper)