Midterm #1

MATH 481/581 — Cryptography
Friday, Feb 16, 2024

Please print your name:

No notes, calculators or tools of any kind are permitted. There are 40 points in total. You need to show work to receive full credit.

Good luck!

Problem 1. (7+1 points) Eve intercepts the ciphertext $c = (111\ 111\ 000)_2$. 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 $m = (010\ 1\ldots)_2$. 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 $\text{PRG} = c \oplus m = (111\ 111\ 000)_2 \oplus (010\ 1\ldots)_2 = (101\ 0\ldots)_2$.

Since each x_n has 3 bits, we learn that $x_1 = (101)_2 = 5$. Using $x_{n+1} \equiv 5x_n + 1 \pmod{8}$, we find $x_2 = 2$, $x_3 = 3$, ... In other words, $\text{PRG} = 5, 2, 3, \ldots = (101\ 010\ 011\ \ldots)_2$.

Hence, Eve can decrypt the ciphertext and obtain $m = c \oplus \text{PRG} = (111\ 111\ 000)_2 \oplus (101\ 010\ 011)_2 = (010\ 101\ 011)_2$.

(b) Unpredictability.

Problem 2. (4 points)

(a) Suppose N is composite. x is a Fermat liar modulo N if and only if $\boxed{}$.

(b) 7 (mod 10) ☐ is a Fermat liar ☐ is not a Fermat liar because $\boxed{}$.

Solution.

(a) x is a Fermat liar modulo N if and only if $x^{N-1} \equiv 1 \pmod{N}$.

(b) 7 is a Fermat liar modulo 10 if and only if $7^9 \equiv 1 \pmod{10}$.

$7^2 \equiv -1 \pmod{10}$, so that $7^8 \equiv 1 \pmod{10}$ and $7^9 \equiv 7 \pmod{10}$. Hence, 7 is not a Fermat liar modulo 10.

Armin Straub
straub@southalabama.edu

Problem 3. (6 points) Using the Chinese remainder theorem, determine all solutions to $x^2 \equiv 4 \pmod{55}$.

Solution. By the CRT:

$$\begin{aligned} & x^2 \equiv 4 \pmod{55} \\ \iff & x^2 \equiv 4 \pmod{5} \text{ and } x^2 \equiv 4 \pmod{11} \\ \iff & x \equiv \pm 2 \pmod{5} \text{ and } x \equiv \pm 2 \pmod{11} \end{aligned}$$

Hence, there are four solutions $\pm 2, \pm a$ modulo 55. To find one of the nontrivial ones, we solve the congruences $x \equiv 2 \pmod{5}$, $x \equiv -2 \pmod{11}$:

$$x \equiv 2 \cdot 11 \cdot \underbrace{11^{-1}_{\operatorname{mod} 5}}_{1} - 2 \cdot 5 \cdot \underbrace{5^{-1}_{\operatorname{mod} 11}}_{-2} \equiv 22 + 20 \equiv -13 \pmod{55}$$

Hence, we conclude that $x^2 \equiv 4 \pmod{55}$ has the four solutions $\pm 2, \pm 13 \pmod{55}$.

Problem 4. (5 points) Evaluate $40^{16011} \pmod{34}$. Show your work!

Solution. First, $40^{16011} \equiv 6^{16011} \pmod{34}$. Since $\phi(34) = \phi(2)\phi(17) = 16$, we have $16011 \equiv 11 \pmod{\phi(34)}$. Combined, we have $40^{16011} \equiv 6^{11} \pmod{34}$.

Using binary exponentiation, we find $6^2 \equiv 2 \pmod{34}$, $6^4 \equiv 2^2 = 4 \pmod{34}$, $6^8 \equiv 4^2 \equiv 16 \pmod{34}$.

In conclusion, $40^{16011} \equiv 6^{11} = 6^8 \cdot 6^2 \cdot 6 \equiv \underbrace{16 \cdot 2}_{\equiv -2} \cdot 6 \equiv -12 \equiv 22 \pmod{34}$.

Problem 5. (2 points) Briefly outline the Fermat primality test.

Solution. Fermat primality test:

Input: number n and parameter k indicating the number of tests to run
Output: "not prime" or "possibly prime"
Algorithm:

Repeat k times:
  Pick a random number a from $\{2, 3, \ldots, n-2\}$.
  If $a^{n-1} \not\equiv 1 \pmod{n}$, then stop and output "not prime".
Output "possibly prime".

Problem 6. (15 points) Fill in the blanks.

(a) $2^{-1} \pmod{29} \equiv$ $\boxed{}$.

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

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

(d) 22 in base 2 is $\boxed{}$.

(e) The residue 10 is invertible modulo n if and only if $\boxed{}$.

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

(g) How many solutions does the congruence $x^2 \equiv 9 \pmod{105}$ have? $\boxed{}$

How many solutions does the congruence $x^2 \equiv 16 \pmod{105}$ have? $\boxed{}$

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

$\boxed{}$

(i) The first 5 bits generated by the Blum-Blum-Shub PRG with $M = 133$ using the seed 5 are $\boxed{}$.

You may use that $16^2 \equiv 123$, $25^2 \equiv 93$, $36^2 \equiv 99$, $92^2 \equiv 85$, $93^2 \equiv 4$, $99^2 \equiv 92 \pmod{133}$.

(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 $\boxed{}$.

(l) The LFSR $x_{n+15} \equiv x_{n+14} + x_n \pmod{2}$ must repeat after $\boxed{}$ 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 $\boxed{}$.

Armin Straub
straub@southalabama.edu

(n) Up to x, there are roughly $\boxed{}$ many primes.

(o) The approximate proportion of primes among numbers up to 2^{1024} is $\boxed{}$. (Simplify!)

Solution.

(a) $2^{-1} \pmod{29} \equiv 15$.

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

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

(d) 22 in base 2 is $(10110)_2$.

(e) The residue 10 is invertible modulo n if and only if $\gcd(10, n) = 1$.

(In other words, 10 is invertible modulo n if and only if n is not a multiple of 2 or 5.)

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

(g) By the CRT, since $105 = 3 \cdot 5 \cdot 7$, the second congruence has $2 \cdot 2 \cdot 2 = 8$ solutions.

The first congruence only has $1 \cdot 2 \cdot 2 = 4$ solutions because $x^2 \equiv 9 \pmod 3$ only has one solution (namely, $x \equiv 0$).

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

(i) The first five bits generated by the Blum-Blum-Shub PRG with $M = 133$ using the seed 5 are $1, 1, 0, 0, 1$ (obtained from $25, 93, 4, 16, 123$).

(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 $x_{n+15} \equiv x_{n+14} + x_n \pmod 2$ must repeat after $2^{15} - 1$ terms.

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

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

(o) By the prime number theorem, there are roughly $2^{1024} / \ln(2^{1024})$ primes up to 2^{1024}. Hence, the proportion of primes among numbers up to 2^{1024} is roughly $\frac{2^{1024} / \ln(2^{1024})}{2^{1024}} = \frac{1}{\ln(2^{1024})} = \frac{1}{1024 \cdot \ln(2)}$.

Comment. $\frac{1}{1024 \cdot \ln(2)} \approx \frac{1}{709.8}$. This means that, roughly, 1 in 710 numbers with 1024 bits is a prime.

(extra scratch paper)