# Midterm #1

Please print your name:

No notes, calculators or tools of any kind are permitted. There are 37 points in total. You need to show work to receive full credit.

### Good luck!

**Problem 1. (6 points)** Eve intercepts the ciphertext  $c = (101 \ 101 \ 011)_2$ . She knows it was encrypted with a stream cipher using the linear congruential generator  $x_{n+1} \equiv 5x_n + 3 \pmod{8}$  as PRG.

Eve further knows that the plaintext begins with  $m = (111 \ 0...)_2$ . Break the cipher and determine the plaintext.

**Solution.** Since  $c = m \oplus PRG$ , we learn that the initial piece of the keystream is  $PRG = m \oplus c = (101\ 101\ 011)_2 \oplus (111\ 0...)_2 = (010\ 1...)_2$ .

Since each  $x_n$  has 3 bits, we learn that  $x_1 = (010)_2 = 2$ . Using  $x_{n+1} \equiv 5x_n + 3 \pmod{8}$ , we find  $x_2 = 5$ ,  $x_3 = 4$ , ... In other words, PRG = 2, 5, 4, ... = (010 \ 101 \ 100 \ ...)\_2.

Hence, Eve can decrypt the ciphertext and obtain  $m = c \oplus PRG = (101\ 101\ 011)_2 \oplus (010\ 101\ 100)_2 = (111\ 000\ 111)_2$ .

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  $x^2 \equiv 16 \pmod{55}$ .

Solution. By the CRT:

 $x^{2} \equiv 16 \pmod{55}$  $\iff x^{2} \equiv 16 \pmod{5} \text{ and } x^{2} \equiv 16 \pmod{11}$  $\iff x \equiv \pm 4 \pmod{5} \text{ and } x \equiv \pm 4 \pmod{11}$ 

Hence, there are four solutions  $\pm 4$ ,  $\pm a$  modulo 55. To find one of the nontrivial ones, we solve the congruences  $x \equiv 4 \pmod{5}$ ,  $x \equiv -4 \pmod{11}$ :

$$x \equiv 4 \cdot 11 \cdot \underbrace{11_{\text{mod}5}^{-1}}_{1} - 4 \cdot 5 \cdot \underbrace{5_{\text{mod}11}^{-1}}_{-2} \equiv 44 + 40 \equiv 29 \equiv -26 \pmod{55}$$

Hence, we conclude that  $x^2 \equiv 16 \pmod{55}$  has the four solutions  $\pm 2, \pm 26 \pmod{55}$ .

### Problem 4. (4 points)

(a) Suppose N is composite. x is a Fermat liar modulo N if and only if

(b) 8 (mod 21)  $\square$  is a Fermat liar because

#### Solution.

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

(b) 8 is a Fermat liar modulo 21 if and only if  $8^{20} \equiv 1 \pmod{21}$ .

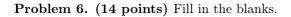
 $8^2 \equiv 1 \pmod{21}$ , so that  $8^{20} \equiv 1 \pmod{21}$ . Hence, 8 a Fermat liar modulo 21.

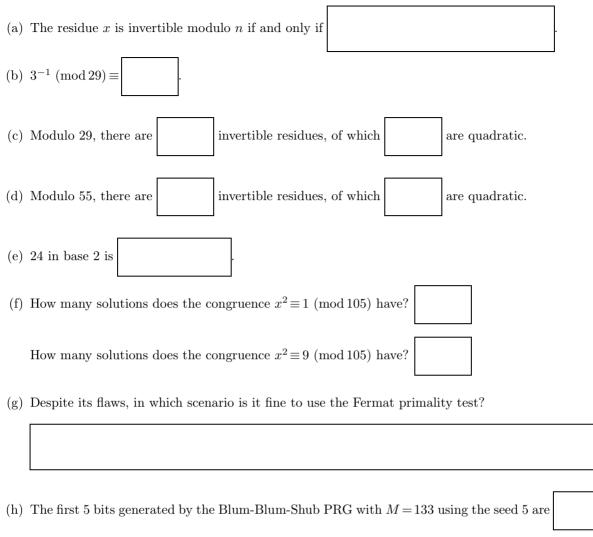
Problem 5. (2 points) Briefly outline the Fermat primality test.

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  $\{2, 3, ..., n-2\}$ . If  $a^{n-1} \not\equiv 1 \pmod{n}$ , then stop and output "not prime". Output "possibly prime".





- You may use that  $16^2 \equiv 123$ ,  $25^2 \equiv 93$ ,  $36^2 \equiv 99$ ,  $92^2 \equiv 85$ ,  $93^2 \equiv 4$ ,  $99^2 \equiv 92 \pmod{133}$ .
- (i) Using a one-time pad and key  $k = (0011)_2$ , the message  $m = (1010)_2$  is encrypted to
- (j) While perfectly confidential, the one-time pad does not protect against
- (k) The LFSR  $x_{n+31} \equiv x_{n+28} + x_n \pmod{2}$  must repeat after

terms.

- (1) Recall that, in a stream cipher, we must never reuse the key stream.Nevertheless, we can reuse the key if we use a
- (m) In order for a PRG to be suitable for use in a stream cipher, the PRG must be

(n) As part of the Miller–Rabin test, it is computed that  $26^{147} \equiv 495$ ,  $26^{294} \equiv 1 \pmod{589}$ .

What do we conclude?

## Solution.

- (a) The residue x is invertible modulo n if and only if gcd(x, n) = 1.
- (b)  $3^{-1} \pmod{29} \equiv 10$
- (c) Modulo the prime 29, there are  $\phi(29) = 28$  invertible residues, of which  $\frac{1}{2}\phi(29) = 14$  are quadratic.
- (d) Modulo 55, there are  $\phi(55) = \phi(5)\phi(11) = 40$  invertible residues, of which  $\frac{1}{4}\phi(55) = 10$  are quadratic.
- (e) 24 in base 2 is  $(11000)_2$ .
- (f) By the CRT, since  $105 = 3 \cdot 5 \cdot 7$ , the first congruence has  $2 \cdot 2 \cdot 2 = 8$  solutions. The second congruence only has  $1 \cdot 2 \cdot 2 = 4$  solutions. (Note that  $x^2 \equiv 9 \pmod{3}$  only has one solution; namely,  $x \equiv 0$ .)
- (g) Despite its flaws, it is fine to use the Fermat primality test for large random numbers.
- (h) 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).
- (i) Using a one-time pad and key  $k = (0011)_2$ , the message  $m = (1010)_2$  is encrypted to  $(1001)_2$ .
- (j) While perfectly confidential, the one-time pad does not protect against tampering.
- (k) The LFSR  $x_{n+31} \equiv x_{n+28} + x_n \pmod{2}$  must repeat after  $2^{31} 1$  terms.
- (l) We can reuse the key if we use a nonce.
- (m) In order for a PRG to be suitable for use in a stream cipher, the PRG must be unpredictable.
- (n) Since  $495 \not\equiv \pm 1 \pmod{589}$ , we conclude that 589 is not a prime.

(extra scratch paper)