Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Score: \_\_\_ / 27

CPSC 42500 Homework 7: Random Number Generation, Primes, Modular Arithmetic

1. (2 pts) If an adversary knows the process by which a 128-bit key was generated, and this process generates keys with only 73 bits of entropy, with what probability can the adversary potentially guess the key (in a single guess)?
2. (2 pts) What is the name of the pseudorandom number generation algorithm used in the random module of the Python standard library? Is this a cryptographically secure PRNG?
3. (3 pts) The Fortuna RNG described in your textbook has been implemented in the Linux operating system. Use the description of its implementation at <https://jlcooke.ca/random/> to answer the following.
	1. Which hash function does it use to extract entropy from input events?
	2. Which block cipher and mode of operation does it use to generate the pseudorandom output?

1. (3 pts) Say an adversary, who does not know the seed of your PRNG, observes the output of one million bits from your generator. They are then able to predict the next bit that will come out with a 51% probability of being correct. Is this PRNG secure enough? Why or why not?
2. (2 pts) Consider the Debian Linux RNG bug described in class, which potentially allowed all SSL traffic coming from the system to be decrypted. How long was the time span between the bug’s introduction and when the vulnerability was announced publicly?
3. (4 pts) Compute the value of the totient function φ for each of the following numbers. Show your work using the method presented in class.

	1. φ(11)
	2. φ(15)
	3. φ(16)
	4. φ(18)

1. (3 pts) Perform the following modular exponentiations using the decomposition method shown in class. Show your work.
	1. 265 (mod 5)
	2. 317 (mod 7)
	3. 419 (mod 11)
2. (5 points) Give the multiplicative inverses of 2, 3, 4, 5, and 6 in the group of multiplication modulo 7. Show the multiplication fact that demonstrates each one.
3. (3 points) Is 5 a generator for the group of multiplication modulo 11? Show why this is or is not the case.