CSE 484 In-section Worksheet #4

Q1. Secret message:

EFVELEQHSCSYFMXICSYVXLYQFEXYWWMV
WEQTWSRMHSFMXIQCXLYQFWMV

ABRAHAMDOYOUBITEYOURTHUMBATUSSIR
SAMPSONIDOBITEMYTHUMBSIR

Q2. Let p = 11. Let g = 10. Compute g^1 mod p, g^2 mod p, g^3 mod p, …, g^{100} mod p.

Look up how to do modular exponentiation if you don't remember!

10 mod 11 = 10
10^2 mod 11 = 1
10^3 mod 11 = 10
10^100 mod 11 = 1

Q3. Let p = 11. Let g = 7. Compute g^1 mod p, g^2 mod p, g^3 mod p, …, g^{100} mod p.

7 mod 11 = 7
7^2 mod 11 = 5
7^3 mod 11 = 2
7^100 mod 11 = 1

Q4. Let p = 11. Let g = 3. Compute g^1 mod p, g^2 mod p, g^3 mod p, …, g^{100} mod p.

3 mod 11 = 3
3^2 mod 11 = 9
3^3 mod 11 = 5
3^100 mod 11 = 1

Q5. Which symmetric encryption mode would you use for the following situations? Why?

You are going to send a small one-time command to fire to your nukes.

A single one time pad would work here.

You are living in the 1970s and want to send a long letter to your lover on ARPANET.

EBC mode with DES

Everything else (given the tools we've learned)

CBC (or CTR) mode with at least AES

Q5. What is a flaw with ECB encryption?

Identical blocks of plaintext produce identical blocks of ciphertext
No integrity checks: can mix and match blocks