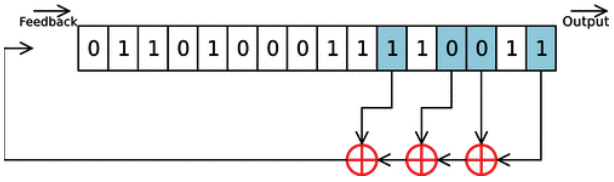
Homework # 2 Due 5pm on Monday Feb 3

CS 178 Intro to Crypto

1. Use the extended Euclid algorithm to compute the inverse of 25 modulo 511.
2. Use the Fermat's Little Theorem to compute the inverse of 2 modulo 47.
3. Use Euler's Theorem to compute the inverse of 81 modulo 323.
4. Determine all invertible elements modulo 48, in $Z_{48}$. Construct the multiplication table of the group consisting these elements and the multiplication operation modulo 48.
5. Compute $\phi(48)$ using the formula given in slides. How does the answer relate to Question 4?
6. Compute $2^{20}$ mod 13 using the binary method.
7. Consider the 5-bit LFSR with connections $c_0 = c_1 = c_2 = c_3 = 1$ and $c_4 = 0$.
   - Given the current state as 10000, compute the next 32 states.
   - Does this 5-bit LFSR cycle through all $2^5 - 1$ states if it starts from a nonzero state?
   - What is the mathematical rule that determines whether or not an $n$-bit LFSR cycles through all $2^n - 1$ nonzero states?
   - What is the definition of maximal LFSR?
   - Is this LFSR maximal?
8. Consider the following LFSR. Given the current state, compute the next 8 states and 8 output bits. It is claimed that this 16-bit LFSR will circulate through all $2^{16} - 1$ states (excluding all zero state). How can you prove this?




Deliver the assignment via Dropbox; link is to be provided. Late submissions are not accepted.