1. (18 points = 10+8) Consider the following “affine” Vigenère cipher: As a key, choose 3 pairs of integers \((a_1, b_1), (a_2, b_2), (a_3, b_3)\), with \(\gcd(a_i, 26) = 1\) for each \(i\). The plaintext letters are represented as integers mod 26. The first letter is encrypted by the affine function \(a_1x + b_1 \mod 26\), the second is encrypted by \(a_2x + b_2 \mod 26\), etc. This is repeated cyclically, so, for example, the 4th, 7th, etc. plaintext letters are encrypted by \(a_1x + b_1 \mod 26\), and the 2nd, 5th, etc. are encrypted by \(a_2x + b_2 \mod 26\).

(a) Explain how to do a chosen plaintext attack on this system. Assume that you know that 3 affine functions are being used.

(b) Suppose we ignore the condition that \(\gcd(a_i, 26) = 1\) and we take \((1, 2), (2, 3), (3, 4)\) as the 3 pairs of our key. Give an example of a ciphertext that has more than one possible decryption, and give two plaintexts that encrypt to this ciphertext.

2. (16 points= 10+6) (a) Suppose you make a modified LFSR machine using the recurrence \(x_{n+2} \equiv A + Bx_n + Cx_{n+1} \mod 2\), where \(A, B, C\) are some constants. Suppose the output sequence starts 0, 1, 1, 0, 0, 1, 1, 0, 0. Find the coefficients \(A, B, C\). Show your work.

(b) Show that the sequence does not satisfy any linear recurrence \(x_{n+2} \equiv c_0x_n + c_1x_{n+1} \mod 2\). One of the following facts might be useful:

\[
\begin{vmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{vmatrix} \equiv 0, \quad \begin{vmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{vmatrix} \equiv 1, \quad \begin{vmatrix} 0 & 1 \\ 1 & 1 \end{vmatrix} \equiv 1.
\]

3. (20 points = 10+10) (a) Find all solutions of \(x^2 \equiv 1 \mod 55\).

(b) Use the fact that \(1852^2 \equiv 3^2 \mod 2279\) to factor 2279. (You must use the given fact; you may not simply try enough factors until you discover the factorization.)

4. (14 points) Let \(p\) and \(q\) be distinct odd primes. It is known that \(a^{(p-1)(q-1)/2} \equiv 1 \mod pq\) whenever \(\gcd(a, pq) = 1\). Suppose that \(d\) and \(e\) are chosen with \(de \equiv 1 \mod (p-1)(q-1)/2\). If Alice has a message \(m\) with \(\gcd(m, pq) = 1\), she encrypts \(m\) as \(c \equiv m^e \mod pq\). Show that \(m \equiv c^d\)
(mod \(pq\)). (You must show explicitly how the fact about \(a^{(p-1)(q-1)/2} \equiv 1 \mod pq\) is used.)

5. (16 points = 8 + 8) A language has two letters, \(A\) and \(B\). The frequency of \(A\) is 80% and the frequency of \(B\) is 20%. You intercept the ciphertext \(BAAABABABA\). It was encrypted by the Vigenère method (where the shifts are mod 2 instead of mod 26).
(a) Suppose you pay a spy $1 million and she tells you the key length is 1, 2, or 3. Show that the key length is probably 2.
(b) Find the plaintext. Explain how you obtained your answer.

6. (16 points: 8 + 8) Alice and Bob play the following game. They choose a large odd integer \(n\) and write \(n - 1 = 2^k m\) with \(m\) odd. Alice then chooses a random integer \(r \neq \pm 1 \mod n\) with \(\gcd(r, n) = 1\). Bob computes \(x_1 \equiv r^m \mod n\). Then Alice computes \(x_2 \equiv x_1^2 \mod n\). Then Bob computes \(x_3 \equiv x_2^2 \mod n\), Alice computes \(x_4 \equiv x_3^2 \mod n\), etc. They stop if someone gets \(\pm 1 \mod n\), and the person who gets \(\pm 1\) wins.
(a) Show that if \(n\) is prime, the game eventually stops.
(b) Suppose \(n\) is the product of two distinct primes and Alice knows this factorization. Show how Alice can choose \(r\) so that she wins on her first play. That is, \(x_1 \neq \pm 1 \mod n\) but \(x_2 \equiv \pm 1 \mod n\).