1. (15 points = 10+5) (a) Let the plaintext be AAAAA. This is the vector (0,0,0,0,0). When this is added to the key vector, the ciphertext is the key. (b) This is a Vigenère system with key length 5.

2. (20 points = 10+10) (a) For each \( n \), use the Fermat test: Calculate \( 2^n - 1 \mod n \). If it is not 1, then \( n \) is not prime. (b) Compute \( \gcd(7172 - 60, 14351) \) using the Euclidean algorithm: \( 14351 = 2 \times 7112 + 127, \) \( 7112 = 56 \times 127 \). The \( \gcd \) is 127 and \( 14351 = 127 \times 113 \).

3. (25 points = 5+10+10) (a) Let \( b_0 = 123456789 \). Let \( b_1 \equiv b_0 \mod 581859289607 \), and \( b_2 \equiv b_2 b_1 \), etc., up to \( b_{16} \equiv b_0 \). This costs 16 cents. Finally, compute \( b_{16} \times b_1 \) to get the answer. The total cost is 17 cents. (b) First find \( d \) using \( d \times 27 \equiv 1 \mod 4 \times 10 \), so \( d = 3 \). Then \( m \equiv c^3 \equiv 48^3 \equiv (-7)^2 \times (-7) \equiv 49 \times (-7) \equiv (-6) \times (-7) \equiv 42 \pmod{55} \). The plaintext is 42. (c) We have \( c \equiv 2718^{301} \equiv (2718^{30})^{10} \times 2718 \equiv 1^{10} \times 2718 \equiv 2718 \).

4. (20 points = 8+7+5) (a) With displacement of 1, there are 4 matches. With a displacement of 2, there are 11 matches. With a displacement of 3, there are 4 matches. So the key length is probably 2. The letters in positions 1, 3, 5, etc. are 8 B’s and 1 A, so they are shifted by 1. The letters in positions 2, 4, 6, etc. are 7 A’s and 1 B, so they are shifted by 0. The key is \{1, 0\}. Shift back by 1 and 0 alternately to obtain AAAAAABAAAAABAAAA
(b) If \( y \equiv 9x + 2 \), then \( 9x \equiv y - 2 \). Multiply by 3 to get \( x \equiv 3y - 6 \) for the decryption function. We have \( G = 6 \rightarrow 3 \times 6 - 6 = 12 \rightarrow M \) and \( M = 12 \rightarrow 3 \times 12 - 6 = 30 \equiv 4 \rightarrow E \). The plaintext is ME.
(c) For example, \( A = 0 \) and \( N = 13 \) both encrypt to \( 1 = B \).

5. (20 points = 15 + 5) (a) (i) affine cipher: If the affine function is \( ax + b \), the ciphertext \( b - a \), repeated many times. This is not enough to determine \( a \) and \( b \). She does not obtain the key. (ii) Vigenère cipher with key length 7: If the key is \( a, b, c, d, e, f, g \), the ciphertext is \( a - 1, b - 1, c - 1, d - 1, e - 1, f - 1, g - 1 \). Eve adds 1 to each and has the key. (iii) Hill cipher with a \( 2 \times 2 \) matrix: If the key is \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \), then the ciphertext is \( (-1, -1) \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (-a - c, -b - d) \), repeated 5 times. This is not enough to determine \( a, b, c, d \), so Eve does not obtain the key. (b) Let \( n = 1 \) to obtain \( x_3 \equiv c_0 x_1 + c_1 x_2 + 1 \), so \( 1 \equiv c_0 + c_1 + 1 \). Similarly, \( n = 2 \) yields \( 0 \equiv c_0 + 1 \). Therefore, \( c_0 = 1 \) and \( c_1 = 0 \).