Problem 1

It can cause 65 bit errors. 64 will be in the current block, and 1 bit in the next block. This is actually one of the main original motivations for CBC mode—i.e. that a single error in transmission does not propagate to too many errors in the output. Therefore, if an error correcting code is wrapped around the outside, it would still have a chance of correcting the error (although it would have to handle the full block error and the additional bit).

Problem 2

A. Let $n = \prod_{i=1}^{i=l} p_i^{k_i}$, where $p_1, \ldots, p_l$ are the prime factors of n. Then, by definition, we have $\phi(n) = \prod_{i=1}^{i=l} p_i^{k_i-1}(p_i - 1)$.

Now, if n has an odd prime factor, then corresponding to that factor p_i, the term $p_i - 1$ in the above product is even, and consequently, $\phi(n)$ is even. Similarly, if n is a power of 2, with the corresponding $k_i > 1$, then the term 2^{k_i-1} is even, so $\phi(n)$ is even.

Thus the only number n for which $\phi(n)$ is odd is 2. The value of $\phi(n)$ in this case is 1. ($n = 1$ is also a valid answer, because $\phi(n)$ can be defined to be 1.)

B. Let $d = \prod_{i=1}^{i=l} p_i^{k_i}$. Then, $m = \prod_{i=1}^{i=l'} p_i^{k'_i}$ with $k'_i \geq k_i, \forall i \leq l$. Now we have $\phi(d) = \prod_{i=1}^{i=l} p_i^{k_i-1}(p_i - 1)$, and $\phi(m) = \prod_{i=1}^{i=l'} p_i^{k'_i-1}(p_i - 1)$. Then, $\phi(m)/\phi(d) = \prod_{i=1}^{i=l} p_i^{k'_i-k_i} \times \prod_{i=l+1}^{i=l'} p_i^{k_i-1}(p_i - 1)$, which is an integer. Thus $\phi(d)|\phi(m)$.

C. Let g be a generator for the group Z_{17}^*. Recall that the group is cyclic. Then, consider the mapping $f(g^a) = a$. Clearly, f maps elements of Z_{17}^* to integers between 0 and 16, that is, elements of the additive group Z_{16}. The mapping is one-to-one and onto, because g is a generator and the group is cyclic; the reverse map is given by $f^{-1}(a) = g^a$.

Let $*$ be the group operation for Z_{17}^*. Now, for two elements g^a and g^b, we have $g^a * g^b = g^{a+b \mod \phi(17)}$ by definition. But, $\phi(17) = 16$. So, $g^a * g^b = g^{a+b \mod 16}$. Thus we have $f(g^a * g^b) = f(a + b)$. This proves that the two groups Z_{17}^* and Z_{16} are isomorphic.

Problem 3

The protocol is given as follows: Alice flips a fair coin and obtains outcome x_A. She uses a bit commitment scheme to commit to the bit x_A and sends the certificate to Bob. Bob then flips a fair coin and obtains outcome x_B. He sends this to Alice. Alice then reveals her bit x_A and proves that this is indeed the bit that she had commited to. Both then compute the result $x = x_A \oplus x_B$.

Note that if both parties are honest, then since x_A and x_B are uniform random bits, their xor is also a uniform random bit, and the protocol succeeds.

Suppose Alice is dishonest while Bob is honest. Assuming that the bit commitment protocol works, Alice cannot influence the outcome after seeing Bob's bit, because she is already committed to x_A. Thus x_A is independent of x_B. Even if x_A is not a fair coin flip (e.g. say it is always 1), the probability that x is 1 is still 0.5, because x_B is a fair coin flip.

Similarly, if Bob is dishonest, while Alice is honest, then x_B is independent of x_A, because after the first step, Bob has no idea about Alice's bit. Thus as before, x is 1 with probability 0.5, and the protocol succeeds.

Problem 4

A. The protocol proceeds in three stages. Alice, Bob and Carol first pick random elements a, b and c. Then, Alice sends $g^a \mod n$ to Bob, Bob sends $g^b \mod n$ to Carol, and Carol sends $g^c \mod n$ to Alice. In the next round, Alice sends $g^{ca} \mod n$ to Bob, Bob sends $g^{ab} \mod n$ to Carol, and Carol sends $g^{bc} \mod n$ to Alice. Finally, the three players compute $g^{abc} \mod n$ and use that as the common secret. This scheme is as secure as the Diffie Hellman scheme for two parties.

B. Both the parties digitally sign their message. In other words, Alice sends $(g^a, E_{r_A}(g^a))$ to Bob, where r_A is Alice's private key. Bob sends $(g^b, E_{r_B}(g^b))$ to Alice, where r_B is his private key. The two parties can verify the sender of the respective messages and thus Mallory cannot impersonate either of them.

Problem 5

A. Knowing e_1 and e_2, Eve first computes r and s such that $re_1 + se_2 = 1$. She can do this by using Euclid's algorithm. Then she computes $m_1^r \times m_2^s = m^{re_1} \times m^{se_2} \mod n = m$.

B. We can assume that N_A, N_B and N_C are coprime, otherwise Eve can factor them and obtain the message m. Now we have $m_A = m^3 \mod N_A$, $m_B = m^3 \mod N_B$, and $m_C = m^3 \mod N_C$. Applying the chinese remainder theorem, Eve can compute $m^3 \mod N_A N_B N_C$, because N_A, N_B and N_C are pairwise coprime. Now, $m < \min(N_A, N_B, N_C)$. So, $m^3 < N_A N_B N_C$, and $m^3 \mod N_A N_B N_C$ is simply m^3. Eve simply takes the cube root of this number and obtains the message m.

Problem 6

For each pair (y, z), Bob can compute the message $m = \frac{z}{y^{11}} \mod (x^3 + 2x + 1)$. This can be done by writing a simple program that computes the inverse of y modulo $x^3 + 2x + 1$, and then computes the product $z \times (y^{-1})^{11} \mod (x^3 + 2x + 1)$.

The question, however, provides us a "trapdoor" that greatly simplifies the calculation, and enables us to find the solution by hand. Recall that x is a generator of the group. For any polynomial y in the group, we can easily compute a such that $x^a = y \mod (x^3 + 2x + 1)$. The respective values are displayed in the table on the next page. Now, for each pair (y, z), we first read off the corresponding a_1 and a_2 from the table. Then, the decoded message is simply $zy^{-11} = x^{a_2 - 11a_1 \mod 26}$. We compute $a_2 - 11a_1 \mod 26$ and read off the corresponding letter from the table below. This gives us the message: GALOISFIELD.

Problem 7

Not written up yet.

A	1	26
B	2	13
C	x	1
D	$1+x$	18
E	$2+x$	11
F	$2x$	14
G	$1+2x$	24
H	$2+2x$	5
I	x^2	2
J	$1+x^2$	7
K	$2+x^2$	3
L	$x+x^2$	19
M	$1+x+x^2$	22
N	$2+x+x^2$	8
O	$2x+x^2$	12
P	$1+2x+x^2$	10
Q	$2+2x+x^2$	4
R	$2x^2$	15
S	$1+2x^2$	16
T	$2+2x^2$	20
U	$x+2x^2$	25
V	$1+x+2x^2$	17
W	$2+x+2x^2$	23
X	$2x+2x^2$	6
Y	$1+2x+2x^2$	21
Z	$2+2x+2x^2$	9

Figure 1: Polynomials and their corresponding logs to base x modulo x^3+2x+1.