1. Recall that C= (P+K) mod 26 and P = (C-K) mod 26, for brute force test possible k values and see if it works. For statistical analysis, count the letters and see which is the most common, then recall e is the most common letter in the alphabet and work form there, answer would be the offset between the index of the two letters . Answer is k=13
   1. Possible number of keys is 2n which is the number of bits in the key . Pr(1 attempt) is 1/n…Pr(2 attempts is (1-1/n) x 1/n-1 = 1/n 🡪 Pr( N-2 attempts) = 1/n. This mans the probability for any number of attempts is 1/n except for n-1 and n as n-1 gives a probability of 2/n as only 2 possible keys are left. It needs 2n-1 attempts on average
   2. B
   3. Statistical analysis
2. For 2^88, we first divide 2^88 by (2^40 \* 2) as we only need to try half of the keys, then we divide by (60 \* 60 \*24 \* 365) to convert tit to years, repeat for other years
3. Perform XOR between plain and cypher
4. It wont be secure as we are using the same key
   1. Since we know P and C, just use P = C XOR K
   2. C`= P’ XOR C XOR P after getting K, then when B decrypts c’ they get P’

* 1. A
  2. Finite state machine so what comes out on what the state of the machine, it only has so many different possibilities
  3. A

1. Make list of all possible binary combinations and calculate for each the probability
   1. In every step, we swap two positions from the identity permutation and as such, no values are gone/replaced
   2. 256! Different permutations in the table and we have 2^8 possible states for and and j thus we multiply all three values for an upper bound
   3. It is relevant because
   4. C0 XOR P0
   5. Given that we know they key, we can perform c’=p’ XOR C XOR P
   6. It will succeed because CRC will change as well and B wont be able to tell
   7. No because we will see that there is a difference between sent MAC and calculated MAC
2. We double the keyspace and thus we get a bigger key and since we 112 bits, harder to crack. We double encrypt (encrypt the encryption). This leads to the issue of D(C,K2) = E(P,K1). We then generate possible values for key combinations for both and then we try find a match. Assuming both are different. However since we change the definition, the issue instead becomes E(C,K2) = E(P,K1), we then repeat the above to find the keys
   1. If plain text is repeated, we would essentially get the same cypher text multiple times which isn’t good and we need different cyphertext values for the same plaintext