SEENG2250 Assignment 1

Harlan De Jong c3349828

Q1

Entire Plaintext:
68656c6c6f746865726569616d74686562657374706572736f6e6576657269686f7065796f75
6861766561676f6f646461797468697369736e69636574657874

Key: C3349828EDEEEFF0F2F3F4F5F7F8F9FA

IV: F7757F821C3A150B605B1BACE4DA03AE

Round 1:

Input of AES: 9F1013EE734E7D6E123E72CD89AE6BCB

Output of AES: e0c24ca1478e1fbdbc6a0f8d4b04c103

Round 2:

Input of AES: 82a73fd537eb6dced3046afb2e76a86b

Output of AES: 4d744bc6a5075aae6b088910f11b6fc6

Round 3:

Input of AES: 22042ebfca7232cf1d6de8779e740ba2

Output of AES: 1ff31f7aa5c37ff7debd61697d6c4a1f

Round 4:

Input of AES: 7e8a6b12ccb01684b0d4020c0909326b

Output of AES: 93730d0cbe92ecada49d26e8bddcc787

Entire Ciphertext:
e0c24ca1478e1fbdbc6a0f8d4b04c1034d744bc6a5075aae6b088910f11b6fc61ff31f7aa5c37ff7
debd61697d6c4a1f93730d0cbe92ecada49d26e8bddcc787

Q2

a,

32^10 possible passwords

b,

Wc = 32^10 / 2000000 = 562949953.4s

Bc = 1 / 2000000 = 0.0000005s

Avg = (Wc+Bc)/2 = 281474976.7s/60/60/24 = 3257.81223 Days

c,

We need to find the unicity distance

U = H(k)/D, where D = 6.

Since there are 32 letters in the alphabet, the total number of keys there can be is 32!

So assuming all keys are equally likely, H(k) = lg(32!) = 117.66

Thus, U = 117.66/6 = 19.61

20 (19.61) characters of given ciphertext means it is in theory possible to identify a unique key

Q3

a,

No, it is and would be extremely difficult for a person to reverse the hash function to find v2 and v1 as it is a one way function which entails it is essentially irreversible. As for finding v4 and v5 from v3 the hash function would need to been known and it states it is secure thus further computation from v3 would be feasibly impossible. Therefore, no other variables in the set can be computed in theory if v3 is known.

b,

No, we cannot use the RSA encryption algorithm as a cryptographic hash function as the primary property of a hash function is that the hash value is fully determined by the data being hashed. In this case it is not 100% determined as the key generation portion of the algorithm happens once and having these same keys is irrespective of the property. Another reason why this will not work is because the algorithm will not uniformly distribute the data across the full set of possible hash values

Q4

a,

Plaintext: in considering time as the fourth dimension more or less equivalent to the three spatial dimensions we run into one rather difficult question

b,

step1: I assumed v = E as v is the most common letter in the ciphertext letter frequency and E is the most common letter in english letter frequency. I used this as a start. (v = E)

step2: I saw multiple occurances of gsv and I assumed this was "THE" as it is a common three letter word ending in E as v = E. With this information I can assume (g = T and s = H)

step3: After changing letters above to the matching ones I have assumed I found a five letter word "THiEE" and here I assume the word is "THREE". thus, (i = R)

step4: With the inclusion of i = R, there was an instance of the text "RzTHER", here I assume the word is "RATHER". Thus, (z = A)

step5: In the current text there was a two letter word "Ah". The most common two letter words that start with "A" is "as" and "at", we already assume g = T from above so it cannot be "at", it must be "as". Thus, (h = S)

step6: After all the assumptions made above we have an instance "oESS" and the only word that comes to mind here is "LESS". Thus, (o = L)

step7: This trend of assuming words continued till all cipher text was decrypted