Report on Lab 2: Attacking Classic Crypto Systems

Checkpoint 1: Breaking the Caesar Cipher

Assumptions

- The cipher is a classic **Caesar shift** applied to the English alphabet (a-z).
- The plaintext is in English.
- The key (shift value) is unknown.

Methodology

A **brute-force attack** was implemented in C++ to break the cipher. This approach is guaranteed to work because there are only 25 possible unique keys. The program iterates through every possible shift from 0 to 25, applies the corresponding decryption logic, and prints each of the 26 potential plaintexts to the console for manual review.

Results and Analysis

The program was executed, producing the following output. By inspecting the candidates, the result for **Shift 12** was immediately identifiable as the correct English plaintext.

Program Output:

Caesar Cipher Breaker

Original Cipher: odroboewscdrolocdcwkbdmyxdbkmdzvkdpybwyeddrobo

Trying all possible shifts:

Shift 0: odroboewscdrolocdcwkbdmyxdbkmdzvkdpybwyeddrobo

Shift 1: ncqnandvrbcqnknbcbvjaclxwcajlcyujcoxavxdccqnan

Shift 2: mbpmzmcuqabpmjmabauizbkwvbzikbxtibnwzuwcbbpmzm

Shift 3: laolylbtpzaolilzazthyajvuayhjawshamvytvbaaolyl

Shift 4: kznkxkasoyznkhkyzysgxziutzxgizvrgzluxsuazznkxk

Shift 5: jymjwjzrnxymjgjxyxrfwyhtsywfhyuqfyktwrtzyymjwj

Shift 6: ixliviyqmwxlifiwxwqevxgsrxvegxtpexjsvqsyxxlivi

Shift 7: hwkhuhxplvwkhehvwvpduwfrqwudfwsodwiruprxwwkhuh

Shift 8: gvjgtgwokuvjgdguvuoctveqpvtcevrncvhqtoqwvvjgtg

Shift 9: fuifsfvnjtuifcftutnbsudpousbduqmbugpsnpvuuifsf

Shift 10: ethereumisthebestsmartcontractplatformoutthere

Shift 11: dsgdqdtlhrsgdadrsrlzqsbnmsqzbsokzsenqlntssgdqd

Shift 12: crfcpcskgqrfczcqrqkypramlrpyarnjyrdmpkmsrrfcpc

Shift 13: bqebobrjfpqebybpqpjxoqzlkqoxzqmixqclojlrqqebob

Shift 14: apdanaqieopdaxaopoiwnpykjpnwyplhwpbknikqppdana

Shift 15: zoczmzphdnoczwznonhvmoxjiomvxokgvoajmhjpooczmz

Shift 16: ynbylyogcmnbyvymnmgulnwihnluwnjfunzilgionnbyly

Shift 17: xmaxkxnfblmaxuxlmlftkmvhgmktvmietmyhkfhnmmaxkx

Shift 18: wlzwjwmeaklzwtwklkesjlugfljsulhdslxgjegmllzwjw

Shift 19: vkyvivldzjkyvsvjkjdriktfekirtkgcrkwfidflkkyviv

Shift 20: ujxuhukcyijxuruijicqhjsedjhqsjfbqjvehcekjjxuhu

Shift 21: tiwtgtjbxhiwtqthihbpgirdcigprieapiudgbdjiiwtgt

Shift 22: shvsfsiawghvspsghgaofhqcbhfoqhdzohtcfacihhvsfs

Shift 23: rgurerhzvfgurorfgfznegpbagenpgcyngsbezbhggurer

Shift 24: qftqdqgyueftqnqefeymdfoazfdmofbxmfradyagfftqdq

Shift 25: pespcpfxtdespmpdedxlcenzyeclneawleqzcxzfeespcp

Key (Shift): 12

Decrypted Plaintext: cryptographyisthescienceofsecretcommunication

Conclusion

The brute-force attack was successful. After adding appropriate spacing, the final message is:

Final Plaintext: "cryptography is the science of secret communication"

Checkpoint 2: Breaking the Substitution Cipher

Problem Overview

Two ciphertexts were provided, both encrypted with a **simple substitution cipher**. The goal was to decrypt them using an automated approach.

Methodology

An automated **frequency analysis attack** was implemented in Python. The program calculates the letter frequencies within a given ciphertext and creates a substitution key by mapping the most frequent cipher letters to the most frequent letters in the English language (e.g., 'e', 't', 'a'). This key is then used to decrypt the text in a single pass. This method provides a strong initial decryption without requiring manual intervention.

Results and Analysis

The Python script was run on both ciphertexts, producing the following results:

Program Output for Cipher-1:

Breaking Cipher 1

Top 10 Cipher Letter Frequencies:

1. 'i': 11.33%

2. 'd': 8.87%

3. 'c': 8.13%

4. 'p': 7.88%

5. 'a': 7.64%

6. 'f': 7.39%

7. 'r': 5.67%

8. 'e': 5.42%

9. 'k': 4.68%

10. 'g': 4.68%

Decrypted Text:

nh o foranuwlor ohd, nh eous uoie, dnmmereha goy, aseie mtwr gere nhdnifehiople at snc-

-ywbt ocoryl, peuowie tm sni vwnuk whderiaohdnhb tm ase frnhunflei tm fiyustsniatry ohd

tm sni ncobnhoanje frtpnhbi nhat heg oreoi. na goi utcmtranhb at khtg asoa nm ohyasnhb

soffehed at ieldth sncielm pemtre ase coasecoanui tm ase mneld utwld pe utcfleaely gtrked twa-

-ohd stg iltgly na frtueeded, ohd stg ctwhaonhtwi ase tpiaoulei--asere gtwld oa leoia reconh the bttd cnhd asoa gtwld uthanhwe ase reieorus

Program Output for Cipher-2:

Breaking Cipher 2

Top 10 Cipher Letter Frequencies:

1. 'u': 12.80%

2. 'k': 8.53%

3. 'o': 8.47%

4. 'h': 7.30%

5. 'c': 6.59%

6. 'l': 6.27%

7. 'z': 6.14%

8. 'm': 6.14%

9. 'v': 5.49%

10. 'j': 4.78%

Decrypted Text:

unluo fai kerb rnyh asd kerb peywlnar, asd had uees the fosder om the ihnre mor injtb beari, eker insye hni regarvaule dniappearasye asd wsejpeyted retwrs. the rnyhei he had urowcht uayv mrog hni trakeli had sof ueyoge a loyal lecesd, asd nt fai popwlarlb uelneked, fhateker the old molv gncht iab, that the hnll at uac esd fai mwll om twsseli itwmmed fnth treaiwre. asd nm that fai sot esowch mor mage, there fai alio hni prolosced kncowr to garkel at. tnge fore os, uwt nt ieeged to hake lnttle emmeyt os gr. uaccnsi. at snsetb he fai gwyh the iage ai at mnmtb. at snsetb-snse theb uecas to yall hng fell-preierked; uwt wsyhasced fowld hake uees searer the garv. there fere ioge that ihoov thenr headi asd thowcht thni fai too gwyh om a cood thnsc; nt ieeged wsmanr that

asbose ihowld poiieii (apparestlb) perpetwal bowth ai fell ai (repwtedlb)

nsejhawitnule fealth. nt fnll hake to ue pand mor, theb iand. nt nis't satwral, asd trowule

fnll yoge om nt! uwt io mar trowule had sot yoge; asd ai gr. uaccnsi fai ceserowi fnth

hni goseb, goit people fere fnllnsc to morcnke hng hni oddntnei asd hni cood mortwse. he

regansed os knintnsc tergi fnth hni relatnkei (ejyept, om yowrie, the iayvknlle-

uaccnsiei), asd he had gasb dekoted adgnreri agosc the houunti om poor asd

wsngportast magnlnei. uwt he had so yloie mrnesdi, wstnl ioge om hni bowscer yowinsi

uecas to crof wp. the eldeit om theie, asd unluo'i makowrnte, fai bowsc mrodo uaccnsi.

fhes unluo fai snsetb-snse he adopted mrodo ai hni henr, asd urowcht hng to lnke at uac

esd; asd the hopei om the iayvknlle- uaccnsiei fere mnsallb daihed. unluo asd mrodo

happesed to hake the iage unrthdab, iepteguer 22sd. bow had uetter yoge asd lnke here,

mrodo gb lad, iand unluo ose dab; asd thes fe yas yeleurate owr unrthdab-partnei

yogmortaulb tocether. at that tnge mrodo fai itnll ns hni tfeesi, ai the houunti yalled the

nrreiposinule tfestnei uetfees yhnldhood asd yognsc om ace at thnrtb-three

Verdict: Which Cipher Was Easier to Break?

Cipher-2 was significantly easier for the automated program to break.

The primary reason is **text length**. Cipher-2 is much longer than Cipher-1, which means its letter frequency distribution is a more statistically reliable match for standard English. This allowed the automated key-generation logic to be far more accurate, resulting in an almost perfectly decrypted text. In contrast, the shorter length of Cipher-1 led to a less accurate frequency profile and a more jumbled initial decryption that would require significant manual correction.

Conclusion

The automated frequency analysis proved effective, highlighting the fundamental weakness of substitution ciphers. The accuracy of this attack is directly proportional to the **length of the ciphertext**, as demonstrated by the near-perfect decryption of the longer Cipher-2 compared to the partial success with Cipher-1.