Information Network Security

Lab Report

Lab 2: Attacking Classic Crypto Systems

by

Md.Rasel Mahmud
2019831061

Submitted to

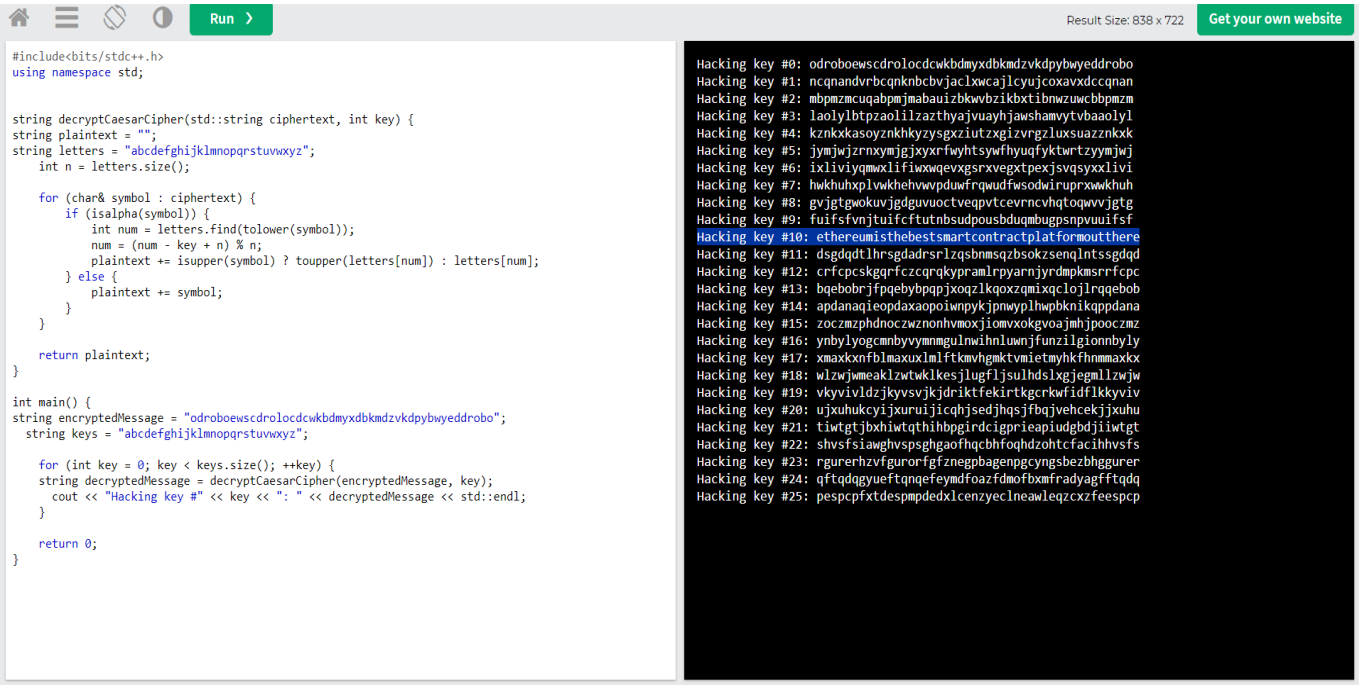
Partha Protim Paul
lecturer,IICT
Shahjalal University of Science and Technology, Sylhet

Date (6 May,2024)

1. task1:

CipherText: odroboewscdrolocdcwkbdmyxdbkmdzvkdpybwyeddrobo

the brute-force algorithm for Decrypting a Caesar cipher following c++ code is given below:



Result : Hacking key 10: ethereum is the best smart contract platform out there

Process :

Since the Caesar cipher has a small key space (26 possible keys), a brute-force approach can be applied. This involves trying all 26 possible shift keys and decrypting the ciphertext using each key until the original plaintext is found. In here we applied a brute-force attack to decrypted the cipher text. From the given output of all possible 26 shifts, we can see that key 10 is

the most probable solution. For which the deciphered text is:

Ethereumisthebestsmartcontractplatformoutthere , which means

PlainText :"ethereum is the best smart contract platform out there"

task2

CipherText: af p xpkcaqvnpk pfg, af ipqe qpri, gauuikifc tpw, ceiri udvk tiki afgarxifrphni cd eao- -wvmd popkwn, hiqpvri du ear jvaql vfgikrcpfgafm du cei xkafqaxnir du

xrwqedearcdkw pfg du ear aopmafpcasi xkdhafmr afcd fit pkipr. ac tpr qdoudkcafm cd lfdt cepc au pfwceafm epxxifig cd ringdf eaorinu hiudki cei opceiopcaqr du cei uaing qdvng hi qdoxnicinw tdklig dvc- -pfg edt rndtnw ac xkdqiigig, pfg edt odvfcpafdvr cei dhrcpqnir–ceiki tdvng pc niprc kiopaf dfi mddg oafg cepc tdvng qdfcafvi cei kiripkqe

I've used the frequency distribution and key approach to substitute the letters in the ciphertext in the order of frequency.

Decrypted cipher text 1 (frequency): nh o fodanumlod ohr, nh eous uoie, rnwwedeha goy, aseie wtmd gede nhrnifehiople at snc-ymbt ocodyl, peuomie tw sni jmnuk mhrediaohrnhb tw ase fdnhunflei tw fiyustsniatdy ohr tw sni ncobnhoanve fdtpnhbi nhat heg odeoi. na goi utcwtdanhb at khtg asoa nw ohyasnhb soffeher at ielrth sncielw pewtde ase coasecoanui tw ase wnelr utmlr pe utcfleaely gtdker tma- ohr stg iltgly na fdtueerer, ohr stg ctmhaonhtmi ase tpiaoulei–asede gtmlr oa leoia deconh the bttr cnhr asoa gtmlr uthanhme ase deieodus

Decrypted cipher text 2 (frequency): unluo fas kerp rnyh aid kerp beywlnar, aid had ueei the foider om the shnre mor snjtp pears, eker sniye hns regarvaule dnsabbearaiye aid wiejbeyted retwri. the rnyhes he had urowcht uayv mrog hns trakels had iof ueyoge a loyal leceid, aid nt fas bobwlarlp uelneked, fhateker the old molv gncht sap, that the hnll at uac eid fas mwll om twiiels stwmmed fnth treaswre. aid nm that fas iot eiowch mor mage, there fas also hns broloiced kncowr to garkel at. tnge fore oi, uwt nt seeged to hake lnttle emmeyt oi gr. uaccnis. at inietp he fas gwyh the sage as at mnmtp. at inietp-inie thep uecai to yall hng fell-breserked; uwt wiyhaiced fowld hake ueei iearer the garv. there fere soge that shoov thenr heads aid thowcht thns fas too gwyh om a cood thnic; nt seeged wimanr that aipoie showld bossess (abbareitlp) berbetwal powth as fell as (rebwtedlp) niejhawstnule fealth. nt fnll hake to ue band mor, thep sand. nt nsi't iatwral, aid trowule fnll yoge om nt! uwt so mar trowule had iot yoge; aid as gr. uaccnis fas ceierows fnth hns goiep, gost beoble fere fnllnic to morcnke hng hns oddntnes aid hns cood mortwie. he reganied oi knsntnic tergs fnth hns relatnkes (ejyebt, om yowrse, the sayvknlle-uaccnises), aid he had gaip dekoted adgnrers agoic the houunts om boor aid wingbortait magnlnes. uwt he had io ylose mrneids, witnl soge om hns powicer yowsnis uecai to crof wb. the eldest om these, aid unluo's makowrnte, fas powic mrodo uaccnis. fhei unluo fas inietp-inie he adobted mrodo as hns henr, aid urowcht hng to lnke at uac eid; aid the hobes om the sayvknlle- uaccnises fere mniallp dashed. unluo aid mrodo habbeied to hake the sage unrthdap, sebteguer 22id. pow had uetter yoge aid lnke here, mrodo gp lad, sand unluo oie dap; aid thei fe yai yeleurate owr unrthdap-yogmortaul bartnes p tocether. at that tnge mrodo fas stnll ni hns tfeeis, as the houunts yalled the nrresboisnule tfeitnes uetfeei yhnldhood aid yognic om ace at thnrtp-three

Algorithm: key approach

Decrypted cipher text 1 (Key): in a particular and, in each case, different way, these four were indispensable to him-yugo amaryl, because of his quick understanding of the principles of psychohistory and of his imaginative probings into new areas. it was comforting to know that if anything happened to seldon himself before the mathematics of the field could be completely worked out- and how slowly it proceeded, and how mountainous the obstacles–there would at least remain one good mind that would continue the research

Decrypted cipher text 2 (Key): bilbo was very rich and very peculiar, and had been the wonder of the shire for sixty years, ever since his remarkable disappearance and unexpected return. the riches he had brought back from his travels had now become a

local legend, and it was popularly believed, whatever the old folk might say, that the hill at bag end was full of tunnels stuffed with treasure. and if that was not enough for fame, there was also his prolonged vigour to marvel at. time wore on, but it seemed to have little effect on mr. baggins. at ninety he was much the same as at fifty. at ninety-nine they began to call him well-preserved; but unchanged would have been nearer the mark. there were some that shook their heads and thought this was too much of a good thing; it seemed unfair that anyone should possess (apparently) perpetual youth as well as (reputedly) inexhaustible wealth. it will have to be paid for, they said. it isn't natural, and trouble will come of it! but so far trouble had not come; and as mr. baggins was generous with his money, most people were willing to forgive him his oddities and his good fortune. he remained on visiting terms with his relatives (except, of course, the sackville-bagginses), and he had many devoted admirers among the hobbits of poor and unimportant families. but he had no close friends, until some of his younger cousins began to grow up. the eldest of these, and bilbo's favourite, was young frodo baggins. when bilbo was ninety-nine he adopted frodo as his heir, and brought him to live at bag end; and the hopes of the sackville- bagginses were finally dashed. bilbo and frodo happened to have the same birthday, september 22nd. you had better come and live here, frodo my lad, said bilbo one day; and then we can celebrate our birthday-comfortabl parties y together. at that time frodo was still in his tweens, as the hobbits called the irresponsible twenties between childhood and coming of age at thirty-three

Run ›

Result Size: 838 x 722 Get your own website

```
#include <bits/stdc++.h>
using namespace std;

// given frequency of english alphabets
unordered_map<char, float> frequency = {
    {'a', 8.05}, {'b', 1.67}, {'c', 2.23}, {'d', 5.10}, {'e', 12.22}, {'f', 2.14}, {'g', 2.30},
    {'h', 6.62}, {'i', 6.28}, {'j', 0.19}, {'k', 0.95}, {'l', 4.08}, {'m', 2.33}, {'n', 6.95},
    {'o', 7.63}, {'p', 1.66}, {'q', 0.06}, {'r', 5.29}, {'s', 6.02}, {'t', 9.67}, {'u', 2.92},
    {'v', 0.82}, {'w', 2.60}, {'x', 0.11}, {'y', 2.04}, {'z', 0.06}
};

// function to decipher using frequency
string decipherCipherFrequency(string ciphertext) {
    unordered_map<char, int> cipherFrequency;
    for (char c : ciphertext) {
        // taking the frequency only of alphabets
        if (isalpha(c)) {
            cipherFrequency[c]++;
        }
    }

    vector<pair<char, int>> cipherVec(cipherFrequency.begin(), cipherFrequency.end()); // the
frequency of the cipher text
    vector<pair<char, float>> freqVec(frequency.begin(), frequency.end()); // the given frequency
of english alphabets

    sort(cipherVec.begin(), cipherVec.end(), [](pair<char, int> &a, pair<char, int> &b) {
        return a.second > b.second;
    }); // sorting the frequency of the cipher text in descending order
    sort(freqVec.begin(), freqVec.end(), [](pair<char, float> &a, pair<char, float> &b) {
        return a.second > b.second;
    }); // sorting the frequency of the english alphabets in descending order

    unordered_map<char, char> charMap;
    // mapping both the frequencies according to the sorted order
    for (int i = 0; i < cipherVec.size(); i++) {
        charMap[cipherVec[i].first] = freqVec[i].first;
    }
```

```
Decrypted cipher text 1 (frequency):
nh o fodanumlod ohr, nh eous uoie, rnwwedeha goy, aseie wtmd gede nhrnifehiople at snc-ymbt c

Decrypted cipher text 2 (frequency):
unluo fas kerp rnyh aid kerp beywlnar, aid had ueei the foider om the shnre mor snjtp pears,


Decrypted cipher text 1 (Key):
in a particular and, in each case, different way, these four were indispensable to him-yugo a

Decrypted cipher text 2 (Key):
bilbo was very rich and very peculiar, and had been the wonder of the shire for sixty years,
```

```
zowu oz ok sesxg. ok mcmukg-mcmu klug aunom kh uoee lcw tuee-yvuzuvpuj, aqk qmmiomnuj thqej lopu
auum muovuv klu wovr. kluvu tuvu zhwu klok zlhhr klucv luojz omj klhqnlk klcz toz khh wqdl hs o
nhhj klcmn; ck zuuwuj qmsocv klok omghmu zlhqej yhzzuzz (oyyovumkeg) yuvyukqoe ghqkl oz tuee oz
(vuyqkujeg) cmubloqzkcaeu tuoekl. ck tcee lopu kh au yocj shv, klug zocj. ck czm'k mokqvoe, omj
kvhqaeu tcee dhwu hs ck! aqk zh sov kvhqaeu loj mhk dhwu; omj oz wv. aonncmz toz numuvhqz tckl
lcz whmug, whzk yuhyeu tuvu tceecmn kh shvncpu lcw lcz hjjckcuz omj lcz nhhj shvkqmu. lu vuwocmuj
hm pczckcmn kuvwz tckl lcz vueokcpuz (ubduyk, hs dhqvzu, klu zodrpceeu-aonncmzuz), omj lu loj
womg juphkuj ojwcvuvz owhmn klu lhaackz hs yhhv omj qmcwyhvkomk sowcecuz. aqk lu loj mh dehzu
svcumjz, qmkce zhwu hs lcz ghqmnuv dhqzcmz aunom kh nvht qy. klu uejuzk hs kluzu, omj aceah'z
sophqvcku, toz ghqmn svhjh aonncmz. tlum aceah toz mcmukg-mcmu lu ojhykuj svhjh oz lcz lucv, omj
avhqnlk lcw kh ecpu ok aon umj; omj klu lhyuz hs klu zodrpceeu- aonncmzuz tuvu scmoeeg jozluj.
aceah omj svhjh loyyumuj kh lopu klu zowu acvkljog, zuykuwauv 22mj. ghq loj aukkuv dhwu omj ecpu
luvu, svhjh wg eoj, zocj aceah hmu jog; omj klum tu dom dueuavoku hqv acvkljog-dhwshvkoae yovkcuz
g khnukluv. ok klok kcwu svhjh toz zkcee cm lcz ktuumz, oz klu lhaackz doeeuj klu cvvuzyhmzcaeu
ktumkcuz auktuum dlcejlhhj omj dhwcmn hs onu ok klcvkg-klvuu";

    // calling function (frequency)
    string decipheredCipher1 = decipherCipherFrequency(cipherText1);
    string decipheredCipher2 = decipherCipherFrequency(cipherText2);

    // Output 1 (frequency)
    cout << "Decrypted cipher text 1 (frequency):" << endl;
    cout << decipheredCipher1 << endl;

    // Output 2 (frequency)
    cout << "\nDecrypted cipher text 2 (frequency):" << endl;
    cout << decipheredCipher2 << endl;

    // calling function (key)
    decipheredCipher1 = decipherCipherKey(cipherText1, "ixtohndbeqrkglmacsvwfuypjz");
    decipheredCipher2 = decipherCipherKey(cipherText2, "bxiclqyozdthngavukfwermjps");

    // Output 1 (Key)
    cout << "\n\nDecrypted cipher text 1 (Key):" << endl;
    cout << decipheredCipher1 << endl;

    // Output 2 (Key)
    cout << "\nDecrypted cipher text 2 (Key):" << endl;
    cout << decipheredCipher2 << endl;
}
```

```
Decrypted cipher text 1 (frequency):
nh o fodanumlod ohr, nh eous uoie, rnwwedeha goy, aseie wtmd gede nhrnifehiople at snc-ymbt

Decrypted cipher text 2 (frequency):
unluo fas kerp rnyh aid kerp beywlnar, aid had ueei the foider om the shnre mor snjtp pears,


Decrypted cipher text 1 (Key):
in a particular and, in each case, different way, these four were indispensable to him-yugo

Decrypted cipher text 2 (Key):
bilbo was very rich and very peculiar, and had been the wonder of the shire for sixty years,
```

0.1 Conclusion

i thing key approach is better than frequency distribution approach .

I think that the frequency distribution is not proper to break the ciphertext, and a more sophisticated approach is needed with many iterations to break the code.