“lrvmnir bpr sumvbwvr jx bpr lmiwv yjeryrkbi jx qmbm wi bpr xjvni mkd ymibrut jx irhx wi bpr riirkvr jx ymbinlmtmipw utn qmumbr dj w ipmhh but bj rhnvwdmbr bpr yjeryrkbi jx bpr qmbm mvvjudwko bj yt wkbrusurbmbwjk lmird jk xjubt trmui jx ibndt
wb wi kjb mk rmit bmiq bj rashmwk rmvp yjeryrkb mkd wbi iwokwxwvmkvr mkd ijyr ynib urymwk nkrashmwkrd bj ower m vjyshrbr rashmkmbwjk jkr cjnhd pmer bj lr fnmhwxwrd mkd wkiswurd bj invp mk rabrkb bpmb pr vjnhd urmvp bpr ibmbr jx rkhwopbrkrd ywkd vmsmlhr jx urvjokwgwko ijnkdhrii ijnkd mkd ipmsrhrii ipmsr w dj kjb drry ytirhx bpr xwkmh mnbpjuwbt lnb yt rasruwrkvr cwbp qmbm pmi hrxb kj djnlb bpmb bpr xjhhjcwko wi bpr sujsru msshwvmbwjk mkd wkbrusurbmbwjk w jxxru yt bprjuwri wk bpr pjsr bpmb bpr riirkvr jx jqwkmcmk qmumbr cwhh urymwk wkbmvb”

Đầu tiên cần phân tích tần suất của bản mã trên bằng đoạn mã nguồn sau:

```
void frequencyAnalysis(std::ifstream& ciphertext)
{
    // Construct frequency map and reverse frequency multimap
    std::map<char,int> freqMap;
    std::multimap<int,char> revFreqMap;
    for (int i = 0; i < 26; ++i)
    {
        freqMap[char(i + 97)] = 0;
    }

    // Find the frequency of all the letters
    char ch;
    while (ciphertext.get(ch))
    {
        if (tolower(ch) >= 'a' && tolower(ch) <= 'z')
        {
            freqMap[ch]++;
        }
    }

    // Swap values and keys in freqMap to revFreqMap
    for (auto elem : freqMap)
    {
        revFreqMap.insert(std::pair<int,char>(elem.second, elem.first));
    }

    // Write to text file
    std::ofstream key ("key.txt");
    for (auto rit = revFreqMap.rbegin(); rit != revFreqMap.rend(); ++rit)
    {
        key << rit->first << rit->second  << std::endl;
    }
    key.close();
}
```

Ta được file key.txt chứa thông tin tần suất xuất hiện các chữ trong bảng mã:

```
84r 68b 62m 49k 48j 47w 41i 30p 24u 23h 23d 22v 20x 19y 17s 17n 13t 8l 7q 7o 5e 5c 5a 1g 1f 0z
```

Tần suất xuất hiện của các chữ trong tiếng Anh là:

E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G	Y	P	B	V	K	J	X	Q	Z

Thay thế ‘r’ bởi ‘e’, ‘b’ bởi ‘t’, ... trong bản mã bằng đoạn mã sau:

```
void replace(std::ifstream& ciphertext, std::ifstream& key)
{
    // Check if the text file can be opened
    if (!key.is_open()) {return;}
    if (!ciphertext.is_open()) {return;}

    // Construct key vector
    std::string line;
    std::vector<char> keyVector (26);
    while (std::getline(key, line))
    {
        keyVector[(int)line[0] - 97] = line[1];
    }

    // Iterate over characters in ciphertext, replace it with key and write to original
    std::ofstream original ("original.txt");
    char ch;
    while (ciphertext.get(ch))
    {
        if (tolower(ch) >= 'a' && tolower(ch) <= 'z')
        {
            original << keyVector[ch - 97];
        }
        else
        {
            original << ch;
        }
    }
    original.close();
}
```

Khóa thay thế (key.txt)

```
re
bt
ma
ko
ji
wn
is
ph
ur
hd
dl
vc
xu
ym
sw
nf
tg
ly
qp
ob
ev
ck
aj
gx
fq
zz
```

Bản mã đã được thay thế (original.txt)

```
yecafse the wractnce iu the yasnc mivemeots iu pata ns
the uicfs aol masterg iu sedu ns the esseoce iu
matsfyagashn rgf parate li n shadd trg ti edfcnlate the
mivemeots iu the pata accirlnob ti mg noterwretatnio
yasel io uirtg gears iu stflg

nt ns oit ao easg tasp ti ejwdano each mivemeot aol nts
snbonuncaoce aol sime mfst remano foejwdanoel ti bnve a
cimwdete ejwdaoatnio ioe kifdl have ti ye qfadnunel aol
noswnrel ti sfch ao ejteot that he cifdl reach the state
iu eodnbhteoel mnol cawayde iu recibonxnob sifoldess
sifol aol shawedess shawe n li oit leem mgsedu the unoad
afthirntg yft mg ejwerneoce knth pata has deut oi lifyt
that the uiddiknob ns the wriwer awwdncatnio aol
noterwretatnio n iuuer mg theirnes no the hiwe that the
esseoce iu ipnoakao parate kndd remano notact
```

Từ đầu tiên ‘yacafse’, rất có thể đây là ‘because’. Ta sửa trong key.txt là ‘ly’ thành ‘lb’, ‘ob’ thành ‘oy’, ‘nf’ thành ‘nu’, ‘xu’ thành ‘xf’. Ta được original.txt mới như sau:

```
because the wractnce if the basnc mivemeots if pata ns
the ficus aol masterg if sedf ns the esseoce if
matsubagashn rgu parate li n shadd trg ti educnlate the
mivemeots if the pata accirlnoy ti mg noterwretatnio
basel io firtg gears if stulg

nt ns oit ao easg tasp ti ejwdano each mivemeot aol nts
snyonfncaoce aol sime must remano uoejwdanoel ti ynve a
cimwdete ejwdaoatnio ioe kiudl have ti be quadnfnel aol
noswnrel ti such ao ejteot that he ciudl reach the state
if eodnyhteoel mnol cawabde if reciyonxnoy siuoldess
siuol aol shawedess shawe n li oit leem mgsedf the fnoad
authirntg but mg ejwerneoce knth pata has deft oi liubt
that the fiddiknoy ns the wriwer awwdncatnio aol
noterwretatnio n iffer mg theirnes no the hiwe that the
esseoce if ipnoakao parate kndd remano notact
```

‘basnc’ trong dòng 1 có thể là ‘basic’, ‘ficus’ trong dòng 2 có thể là ‘focus’. Tiếp tục sửa trong key.txt như sau: ‘wn’ thành ‘wi’, ‘ji’ thành ‘jo’, ‘ko’ thành ‘kn’. Ta được:

```
because the wractice of the basic movements of pata is
the focus anl masterg of sedf is the essence of
matsubagashi rgu parate lo i shadd trg to educilate the
movements of the pata accorliny to mg interwretation
basel on fortg gears of stulg

it is not an easg tasp to ejwdain each movement anl its
siynificance anl some must remain unejwdainel to yive a
comwdete ejwdanation one koudl have to be quadifiel anl
inswirel to such an ejtent that he coudl reach the state
of endiyhtenel minl cawabde of recoynixiny sounldess
sounl anl shawedess shawe i lo not leem mgsedf the finad
authoritg but mg ejwerience kith pata has deft no loubt
that the foddokiny is the wrower awwdication anl
interwretation i offer mg theories in the howe that the
essence of opinakan parate kidd remain intact
```

‘easg tasp’ ở đoạn 2 dòng 1 có thể là ‘easy task’, ‘coudl’ ở dòng 4 đoạn 2 có thể là ‘could’, ‘mg ejwerience’ ở dòng 7 đoạn 2 có thể là ‘my experience’. Thay thế trong key.txt như sau: ‘tg’ thành ‘ty’, ‘oy’ thành ‘og’, ‘qp’ thành ‘qk’, ‘ck’ thành ‘cp’, ‘hd’ thành ‘hl’, ‘dl’ thành ‘dd’, ‘aj’ thành ‘ax’, ‘gx’ thành ‘gj’, ‘sw’ thành ‘sp’, ‘cp’ thành ‘cw’.

Bản giải mã mới như sau:

```
because the practice of the basic movements of kata is
the focus and mastery of self is the essence of
matsubayashi ryu karate do i shall try to elucidate the
movements of the kata according to my interpretation
based on forty years of study

it is not an easy task to explain each movement and its
significance and some must remain unexplained to give a
complete explanation one would have to be qualified and
inspired to such an extent that he could reach the state
of enlightened mind capable of recognijing soundless
sound and shapeless shape i do not deem myself the final
authority but my experience with kata has left no doubt
that the following is the proper application and
interpretation i offer my theories in the hope that the
essence of okinawan karate will remain intact
```

‘recognijing’ ở hàng 5 đoạn 2 chính là ‘recognizing’. Ta sửa trong key.txt: ‘gj’ thành ‘gz’ và ‘zz’ thành ‘zj’. Văn bản được giải mã hoàn chỉnh như sau:

```
because the practice of the basic movements of kata is
the focus and mastery of self is the essence of
matsubayashi ryu karate do i shall try to elucidate the
movements of the kata according to my interpretation
based on forty years of study

it is not an easy task to explain each movement and its
significance and some must remain unexplained to give a
complete explanation one would have to be qualified and
inspired to such an extent that he could reach the state
of enlightened mind capable of recognizing soundless
sound and shapeless shape i do not deem myself the final
authority but my experience with kata has left no doubt
that the following is the proper application and
interpretation i offer my theories in the hope that the
essence of okinawan karate will remain intact
```

Văn bản được **Shōshin Nagamine** viết trong **The Essence of Okinawan Karate-Do**. Khóa thay thế hoàn chỉnh:

```
re
bt
ma
kn
jo
wi
is
ph
ur
hl
dd
vc
xf
ym
sp
nu
ty
lb
qk
og
ev
cw
ax
gz
fq
zj
```