**Bài Tập 1**

**Họ và tên: Phạm Văn Nam**

**MSSV: 20183599**

1. Tần suất của các kí tự trong đoạn ciphertext:

|  |  |  |  |
| --- | --- | --- | --- |
| Kí tự | Tần suất (%) | Kí tự | Tần suất (%) |
| a | 0.77 | n | 2.63 |
| b | 10.53 | o | 1.08 |
| c | 0.77 | p | 4.64 |
| d | 3.56 | q | 1.08 |
| e | 0.77 | r | 13.0 |
| f | 0.15 | s | 2.63 |
| g | 0.15 | t | 2.01 |
| h | 3.56 | u | 3.72 |
| i | 6.35 | v | 3.41 |
| j | 7.43 | w | 7.28 |
| k | 7.59 | x | 3.10 |
| l | 1.24 | y | 2.94 |
| m | 9.60 | z | 0.00 |

1. Giải mã đoạn text:

Em thực hiện sắp xếp lại thứ tự các kí tự theo tần suất:

|  |  |  |
| --- | --- | --- |
| Thứ tự | Kí tự tiếng Anh | Kí tự trong đoạn ciphertext |
| 1 | e | r |
| 2 | t | b |
| 3 | a | m |
| 4 | o | k |
| 5 | i | j |
| 6 | n | w |
| 7 | s | i |
| 8 | h | p |
| 9 | r | u |
| 10 | d | h |
| 11 | l | d |
| 12 | c | v |
| 13 | u | x |
| 14 | m | y |
| 15 | w | s |
| 16 | f | n |
| 17 | g | t |
| 18 | y | l |
| 19 | p | q |
| 20 | b | o |
| 21 | v | e |
| 22 | k | c |
| 23 | x | a |
| 24 | j | g |
| 25 | q | f |
| 26 | z | z |

Sau đó thay thế các kí tự trong ciphertext bằng các kí tự tương ứng như bảng tần suất bên trên, thu được đoạn text sau:

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 EXWDANO EACH MIVEMEOT AOL NTS

SNBONUNCAOCE AOL SIME MFST REMANO FOEXWDANOEL TI BNVE A

CIMWDETE EXWDAOATNIO IOE KIFDL HAVE TI YE QFADNUNEL AOL

NOSWNREL TI SFCH AO EXTEOT THAT HE CIFDL REACH THE STATE

IU EODNBHTEOEL MNOL CAWAYDE IU RECIBONJNOB SIFOLDESS

SIFOL AOL SHAWEDESS SHAWE N LI OIT LEEM MGSEDU THE UNOAD

AFTHIRNTG YFT MG EXWERNEOCE 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 đoạn text này, em thấy một vài từ tiếng Anh xuất hiện: the, that, have, state, reach, has. Em đoán được những kí tự đã đúng là: t, h, a, e, s, r, tương ứng là các kí tự b, p, m, r, i, u trong đoạn ciphertext. Sau đó em chỉ thay những kí tự này vào ciphertext, thu được đoạn text sau (các kí tự được in hoa là các kí tự đã được thay thế, kí tự in thường là kí tự gốc trong ciphertext):

lEvAnSE THE sRAvTwvE jx THE lASwv yjeEyEkTS jx qATA wS

THE xjvnS Akd yASTERt jx SEhx wS THE ESSEkvE jx

yATSnlAtASHw Rtn qARATE dj w SHAhh TRt Tj EhnvwdATE THE

yjeEyEkTS jx THE qATA AvvjRdwko Tj yt wkTERsRETATwjk

lASEd jk xjRTt tEARS jx STndt

wT wS kjT Ak EASt TASq Tj EashAwk EAvH yjeEyEkT Akd wTS

SwokwxwvAkvE Akd SjyE ynST REyAwk nkEashAwkEd Tj oweE A

vjyshETE EashAkATwjk jkE cjnhd HAeE Tj lE fnAhwxwEd Akd

wkSswREd Tj SnvH Ak EaTEkT THAT HE vjnhd REAvH THE STATE

jx EkhwoHTEkEd ywkd vAsAlhE jx REvjokwgwko SjnkdhESS

Sjnkd Akd SHAsEhESS SHAsE w dj kjT dEEy ytSEhx THE xwkAh

AnTHjRwTt lnT yt EasERwEkvE cwTH qATA HAS hExT kj djnlT

THAT THE xjhhjcwko wS THE sRjsER AsshwvATwjk Akd

wkTERsRETATwjk w jxxER yt THEjRwES wk THE HjsE THAT THE

ESSEkvE jx jqwkAcAk qARATE cwhh REyAwk wkTAvT

Trong đoạn text, xuất hiện nhiều lần các từ wS, wT, wTS => em đoán các từ này là it, is, its, nên em tiếp tục thay thế w = I và được văn bản sau:

lEvAnSE THE sRAvTIvE jx THE lASIv yjeEyEkTS jx qATA IS

THE xjvnS Akd yASTERt jx SEhx IS THE ESSEkvE jx

yATSnlAtASHI Rtn qARATE dj I SHAhh TRt Tj EhnvIdATE THE

yjeEyEkTS jx THE qATA AvvjRdIko Tj yt IkTERsRETATIjk

lASEd jk xjRTt tEARS jx STndt

IT IS kjT Ak EASt TASq Tj EashAIk EAvH yjeEyEkT Akd ITS

SIokIxIvAkvE Akd SjyE ynST REyAIk nkEashAIkEd Tj oIeE A

vjyshETE EashAkATIjk jkE cjnhd HAeE Tj lE fnAhIxIEd Akd

IkSsIREd Tj SnvH Ak EaTEkT THAT HE vjnhd REAvH THE STATE

jx EkhIoHTEkEd yIkd vAsAlhE jx REvjokIgIko SjnkdhESS

Sjnkd Akd SHAsEhESS SHAsE I dj kjT dEEy ytSEhx THE xIkAh

AnTHjRITt lnT yt EasERIEkvE cITH qATA HAS hExT kj djnlT

THAT THE xjhhjcIko IS THE sRjsER AsshIvATIjk Akd

IkTERsRETATIjk I jxxER yt THEjRIES Ik THE HjsE THAT THE

ESSEkvE jx jqIkAcAk qARATE cIhh REyAIk IkTAvT

Trong đoạn text xuất hiện các từ qATA, qARATE, TASq => em đoán các từ này là kata, karate, task, nên em thay thế q = K, tiếp tục thu được đoạn text:

lEvAnSE THE sRAvTIvE jx THE lASIv yjeEyEkTS jx KATA IS

THE xjvnS Akd yASTERt jx SEhx IS THE ESSEkvE jx

yATSnlAtASHI Rtn KARATE dj I SHAhh TRt Tj EhnvIdATE THE

yjeEyEkTS jx THE KATA AvvjRdIko Tj yt IkTERsRETATIjk

lASEd jk xjRTt tEARS jx STndt

IT IS kjT Ak EASt TASK Tj EashAIk EAvH yjeEyEkT Akd ITS

SIokIxIvAkvE Akd SjyE ynST REyAIk nkEashAIkEd Tj oIeE A

vjyshETE EashAkATIjk jkE cjnhd HAeE Tj lE fnAhIxIEd Akd

IkSsIREd Tj SnvH Ak EaTEkT THAT HE vjnhd REAvH THE STATE

jx EkhIoHTEkEd yIkd vAsAlhE jx REvjokIgIko SjnkdhESS

Sjnkd Akd SHAsEhESS SHAsE I dj kjT dEEy ytSEhx THE xIkAh

AnTHjRITt lnT yt EasERIEkvE cITH KATA HAS hExT kj djnlT

THAT THE xjhhjcIko IS THE sRjsER AsshIvATIjk Akd

IkTERsRETATIjk I jxxER yt THEjRIES Ik THE HjsE THAT THE

ESSEkvE jx jKIkAcAk KARATE cIhh REyAIk IkTAvT

Trong đoạn text, xuất hiện các từ EASt, TRt, tEARS => em đoán các từ này là easy, try, years, nên em thay thế t = Y, sau đó thu được đoạn text:

lEvAnSE THE sRAvTIvE jx THE lASIv yjeEyEkTS jx KATA IS

THE xjvnS Akd yASTERY jx SEhx IS THE ESSEkvE jx

yATSnlAYASHI RYn KARATE dj I SHAhh TRY Tj EhnvIdATE THE

yjeEyEkTS jx THE KATA AvvjRdIko Tj yY IkTERsRETATIjk

lASEd jk xjRTY YEARS jx STndY

IT IS kjT Ak EASY TASK Tj EashAIk EAvH yjeEyEkT Akd ITS

SIokIxIvAkvE Akd SjyE ynST REyAIk nkEashAIkEd Tj oIeE A

vjyshETE EashAkATIjk jkE cjnhd HAeE Tj lE fnAhIxIEd Akd

IkSsIREd Tj SnvH Ak EaTEkT THAT HE vjnhd REAvH THE STATE

jx EkhIoHTEkEd yIkd vAsAlhE jx REvjokIgIko SjnkdhESS

Sjnkd Akd SHAsEhESS SHAsE I dj kjT dEEy yYSEhx THE xIkAh

AnTHjRITY lnT yY EasERIEkvE cITH KATA HAS hExT kj djnlT

THAT THE xjhhjcIko IS THE sRjsER AsshIvATIjk Akd

IkTERsRETATIjk I jxxER yY THEjRIES Ik THE HjsE THAT THE

ESSEkvE jx jKIkAcAk KARATE cIhh REyAIk IkTAvT

Lặp lại quá trình trên cho đến khi giải được hết tất cả các kí tự, em thu được khóa như sau:

E = r, T = b, A = m, O = j, I = w, N = k, S = i, H = p, R = u, D = d, L = h, C = v, U = n, M = y, W = c, F = x, G = o, Y = t, P = s, B = l, V = e, K = q, X = a, J = g, Q = f, Z = g

(Kí tự in hoa là kí tự thay thế, kí tự in thường là kí tự gốc trong ciphertext )

Và đoạn text được giải mã hoàn chỉnh:

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

1. Người đã viết đoạn văn bản này là Shoshun Nagamine.