BAHCESEHIR UNIVERSITY

CMP5121

–

NETWORK SECURITY AND CRYPTOGRAPHY

HOMEWORK #1

Eser İnan Arslan – 1905482

1)

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

\*\*\* r -> E, b -> T, m -> A

lEvAniE TpE suAvTwvE jx TpE lAiwv yjeEyEkTi jx qATA wi

TpE xjvni Akd yAiTEut jx iEhx wi TpE EiiEkvE jx

yATinlAtAipw utn qAuATE dj w ipAhh Tut Tj EhnvwdATE TpE

yjeEyEkTi jx TpE qATA Avvjudwko Tj yt wkTEusuETATwjk

lAiEd jk xjuTt tEAui jx iTndt

wT wi kjT Ak EAit TAiq Tj EashAwk EAvp yjeEyEkT Akd wTi

iwokwxwvAkvE Akd ijyE yniT uEyAwk nkEashAwkEd Tj oweE A

vjyshETE EashAkATwjk jkE cjnhd pAeE Tj lE fnAhwxwEd Akd

wkiswuEd Tj invp Ak EaTEkT TpAT pE vjnhd uEAvp TpE iTATE

jx EkhwopTEkEd ywkd vAsAlhE jx uEvjokwgwko ijnkdhEii

ijnkd Akd ipAsEhEii ipAsE w dj kjT dEEy ytiEhx TpE xwkAh

AnTpjuwTt lnT yt EasEuwEkvE cwTp qATA pAi hExT kj djnlT

TpAT TpE xjhhjcwko wi TpE sujsEu AsshwvATwjk Akd

wkTEusuETATwjk w jxxEu yt TpEjuwEi wk TpE pjsE TpAT TpE

EiiEkvE jx jqwkAcAk qAuATE cwhh uEyAwk wkTAvT

\*\*\* v => C

lECAniE THE suACTICE OF THE lAiIC yOeEyENTi OF qATA Ii

THE FOCni AND yAiTEut OF iEhF Ii THE EiiENCE OF

yATinlAtAiHI utn qAuATE DO I iHAhh Tut TO EhnCIDATE THE

yOeEyENTi OF THE qATA ACCOuDINo TO yt INTEusuETATION

lAiED ON FOuTt tEAui OF iTnDt

IT Ii NOT AN EAit TAiq TO EashAIN EACH yOeEyENT AND ITi

iIoNIFICANCE AND iOyE yniT uEyAIN nNEashAINED TO oIeE A

COyshETE EashANATION ONE cOnhD HAeE TO lE fnAhIFIED AND

INisIuED TO inCH AN EaTENT THAT HE COnhD uEACH THE iTATE

OF ENhIoHTENED yIND CAsAlhE OF uECOoNIgINo iOnNDhEii

iOnND AND iHAsEhEii iHAsE I DO NOT DEEy ytiEhF THE FINAh

AnTHOuITt lnT yt EasEuIENCE cITH qATA HAi hEFT NO DOnlT

THAT THE FOhhOcINo Ii THE suOsEu AsshICATION AND

INTEusuETATION I OFFEu yt THEOuIEi IN THE HOsE THAT THE

EiiENCE OF OqINAcAN qAuATE cIhh uEyAIN INTACT

\*\*\* i => S , n => U

lECAUSE THE suACTICE OF THE lASIC yOeEyENTS OF qATA IS

THE FOCUS AND yASTEut OF SEhF IS THE ESSENCE OF

yATSUlAtASHI utU qAuATE DO I SHAhh Tut TO EhUCIDATE THE

yOeEyENTS OF THE qATA ACCOuDINo TO yt INTEusuETATION

lASED ON FOuTt tEAuS OF STUDt

IT IS NOT AN EASt TASq TO EashAIN EACH yOeEyENT AND ITS

SIoNIFICANCE AND SOyE yUST uEyAIN UNEashAINED TO oIeE A

COyshETE EashANATION ONE cOUhD HAeE TO lE fUAhIFIED AND

INSsIuED TO SUCH AN EaTENT THAT HE COUhD uEACH THE STATE

OF ENhIoHTENED yIND CAsAlhE OF uECOoNIgINo SOUNDhESS

SOUND AND SHAsEhESS SHAsE I DO NOT DEEy ytSEhF THE FINAh

AUTHOuITt lUT yt EasEuIENCE cITH qATA HAS hEFT NO DOUlT

THAT THE FOhhOcINo IS THE suOsEu AsshICATION AND

INTEusuETATION I OFFEu yt THEOuIES IN THE HOsE THAT THE

ESSENCE OF OqINAcAN qAuATE cIhh uEyAIN INTACT

\*\*\* l => B, h => L, t => Y, u => R, y => M,

BECAUSE THE sRACTICE OF THE BASIC MOeEMENTS OF qATA IS

THE FOCUS AND MASTERY OF SELF IS THE ESSENCE OF

MATSUBAYASHI RYU qARATE DO I SHALL TRY TO ELUCIDATE THE

MOeEMENTS OF THE qATA ACCORDINo TO MY INTERsRETATION

BASED ON FORTY YEARS OF STUDY

IT IS NOT AN EASY TASq TO EasLAIN EACH MOeEMENT AND ITS

SIoNIFICANCE AND SOME MUST REMAIN UNEasLAINED TO oIeE A

COMsLETE EasLANATION ONE cOULD HAeE TO BE fUALIFIED AND

INSsIRED TO SUCH AN EaTENT THAT HE COULD REACH THE STATE

OF ENLIoHTENED MIND CAsABLE OF RECOoNIgINo SOUNDLESS

SOUND AND SHAsELESS SHAsE I DO NOT DEEM MYSELF THE FINAL

AUTHORITY BUT MY EasERIENCE cITH qATA HAS LEFT NO DOUBT

THAT THE FOLLOcINo IS THE sROsER AssLICATION AND

INTERsRETATION I OFFER MY THEORIES IN THE HOsE THAT THE

ESSENCE OF OqINAcAN qARATE cILL REMAIN INTACT

\*\*\* e => V, s => P, a => X, o => G

BECAUSE THE PRACTICE OF THE BASIC MOVEMENTS OF qATA IS

THE FOCUS AND MASTERY OF SELF IS THE ESSENCE OF

MATSUBAYASHI RYU qARATE DO I SHALL TRY TO ELUCIDATE THE

MOVEMENTS OF THE qATA ACCORDING TO MY INTERPRETATION

BASED ON FORTY YEARS OF STUDY

IT IS NOT AN EASY TASq TO EXPLAIN EACH MOVEMENT AND ITS

SIGNIFICANCE AND SOME MUST REMAIN UNEXPLAINED TO GIVE A

COMPLETE EXPLANATION ONE cOULD HAVE TO BE fUALIFIED AND

INSPIRED TO SUCH AN EXTENT THAT HE COULD REACH THE STATE

OF ENLIGHTENED MIND CAPABLE OF RECOGNIgING SOUNDLESS

SOUND AND SHAPELESS SHAPE I DO NOT DEEM MYSELF THE FINAL

AUTHORITY BUT MY EXPERIENCE cITH qATA HAS LEFT NO DOUBT

THAT THE FOLLOcING IS THE PROPER APPLICATION AND

INTERPRETATION I OFFER MY THEORIES IN THE HOPE THAT THE

ESSENCE OF OqINAcAN qARATE cILL REMAIN INTACT

\*\*\* f => Q, g => Z, q => K, c => W

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

A screenshot of a social media post

Description automatically generated

A screenshot of a social media post

Description automatically generated

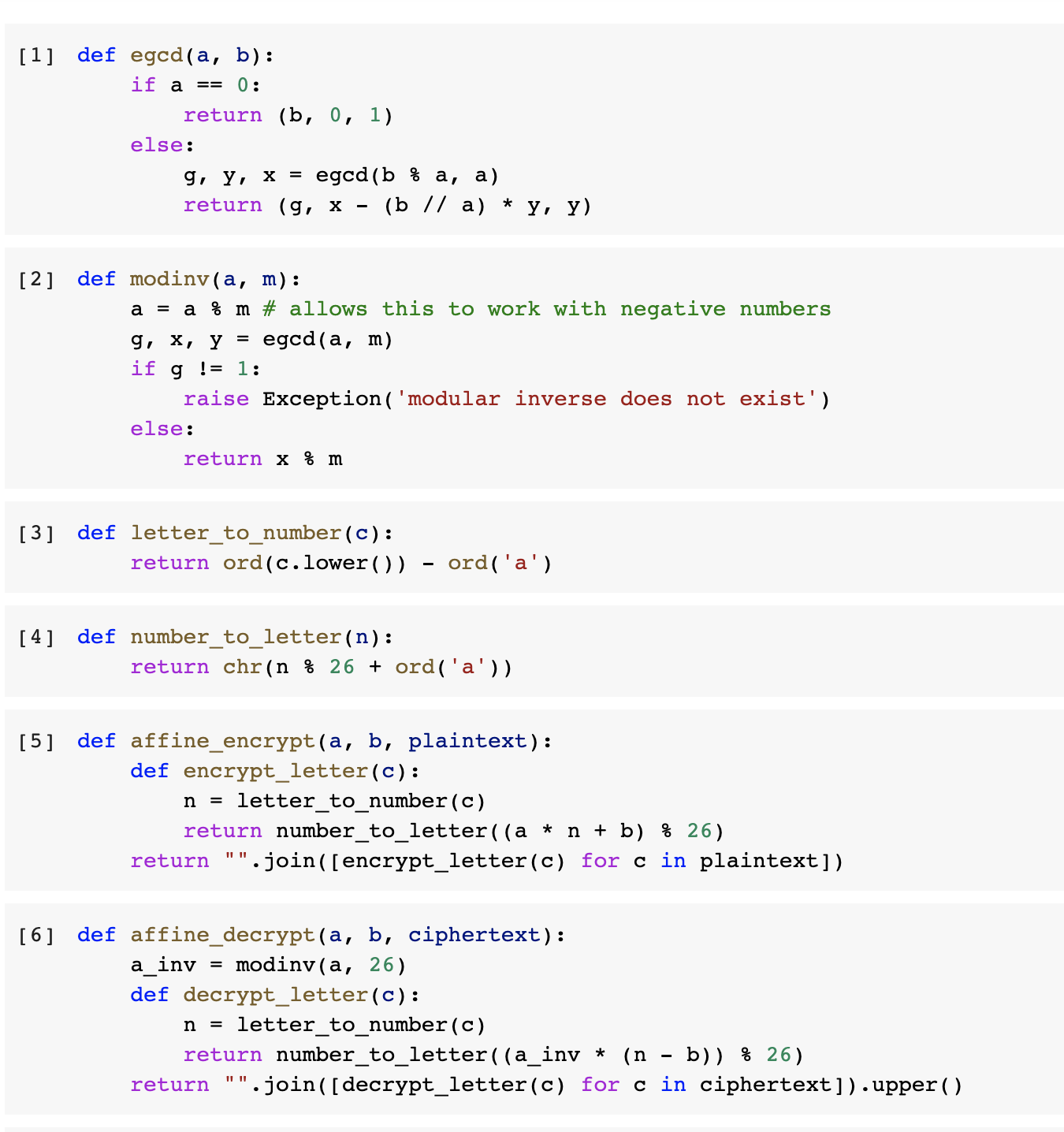
A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

2)



A screenshot of a social media post

Description automatically generated

===========

Ciphertext:

===========

falszztysyjzyjkywjrztyjztyynaryjkyswarztyegyyj

====================================

Plaintext (as decrypted by (7, 22)):

====================================

FIRSTTHESENTENCEANDTHENTHEEVIDENCESAIDTHEQUEEN

3)

A close up of a whiteboard

Description automatically generated

a.

S2 S1 S0 OUTPUT

1 0 0 0

1 1 0 0

1 1 1 1

0 1 1 1

1 0 1 1

0 1 0 0

0 0 1 1

1 0 0 0 \*\*\*\*\*\*

b.

S2 S1 S0 OUTPUT

0 1 1 1

1 0 1 1

0 1 0 0

0 0 1 1

1 0 0 0

1 1 0 0

1 1 1 1

0 1 1 1 \*\*\*\*\*\*

c. Since (0,1,1) is part of the sequence for (1,0,0), its loop is exactly the same, but rotated back by three positions. Both of them give the same loop of states (which contains of all non-zero 3-bit binary numbers), but starting from whatever was chosen to initialise it.

4) X8 + X4 + X2 + X + 1(Polynomial)

A close up of text on a whiteboard

Description automatically generated

S7 S6 S5 S4 S3 S2 S1 S0 OUTPUT

1 1 1 1 1 1 1 1 1

0 1 1 1 1 1 1 1 1

0 0 1 1 1 1 1 1 1

0 0 0 1 1 1 1 1 1

0 0 0 0 1 1 1 1 1

1 0 0 0 0 1 1 1 1

1 1 0 0 0 0 1 1 1

0 1 1 0 0 0 0 1 1

1 0 1 1 0 0 0 0 0

1 1 0 1 1 0 0 0 0

1 1 1 0 1 1 0 0 0

1 1 1 1 0 1 1 0 0

1 1 1 1 1 0 1 1 1

1 1 1 1 1 1 0 1 1

1 1 1 1 1 1 1 0 0

1 1 1 1 1 1 1 1 1

The result of 1011000011111111(2) is equal to B0FF(16)