Abel Marin

Prof Joe

Cryptology

April 12, 2020

Assignment 1

1. Problem 1
   1. Letter frequency: a: 5, b: 68, c: 5, d: 23, e: 5, f: 1, g: 1, h: 23, i: 41, j: 48, k: 49, l: 8, m: 62, n: 17, o: 7, p: 30, q: 7, r: 84, s: 17, t: 13, u: 24, v: 22, w: 47, x: 20, y: 19, z: 0
   2. 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. It seems like this is from The Essence of Okinawan Karate-Do by Shoshin Nagamine.

1. Problem 2
   1. We start by calculating 15 = 1\*13+2 thus 15 = 2 mod 13 and 29 = 2\*13+3 thus 29 = 3 mod 13. Next multiply 2\*3 = 6 and 0 <= 6 < 13. **Answer: 15\*29 mod 13 = 6 mod 13**
   2. We begin by calculating 29 = 2\*13+3 thus 29 = 3 mod 13. Next we multiply 2\*3 = 6 which 0 <= 6 < 13. **Answer: 2\*29 mod 13 = 6 mod 13**
   3. We simply multiply 2\*3 and get 6 and 0 <= 6 < 13. **Answer: 2\*3 mod 13 = 6 mod 13**.
   4. We begin by computing -11 = -1\*13+2 thus -11 = 2 mod 13. Next we multiply 2\*3 = 6 which 0 <= 6 < 13. **Answer: -11\*3 mod 13 = 6 mod 13**.
   5. In order to find the multiplicative inverse, we start by setting x = 1/5mod13. We then multiply by 5 on both sides 5x = 1mod13. Next, we brute force find an x and we get 8; 5\*8 mod 13 = 40 mod 13 = 1 mod 13. **Answer: 8**.
   6. In order to find the multiplicative inverse, we start by setting x = 1/5mod7. We then multiply by 5 on both sides 5x = 1mod7. Next, we brute force find an x and we get 3; 5\*3 mod 7 = 15 mod 7 = 1 mod 7. **Answer: 3**.
   7. In order to find the multiplicative inverse, we begin by simplifying by multiplying 3\*2 = 6. We next set x = 6/5mod7. We then multiply by 5 on both sides 5x = 6mod7. Next, we brute force find an x and we get 4; 5\*4 mod 7 = 20 mod 7 = 6 mod 7. **Answer: 4**.
2. Problem 3
   1. (program on a1\_abelmarin.py)
   2. The most likely answer seems to be gjccz means “hello” at a-1 = 25 and -b = 13. However there were a few results which are words but which I doubt to be the actually answer including “comma” at a-1: 4, -b: 1 & a-1: 4, -b: 14 and “duppy” at a-1: 23, -b: 19. I will stick by my answer that gjccz is the cyphertext for hello at a-1 = 25 and -b = 13.
   3. This is every single possible a-1 and -b outputted by a1\_abelmarin.py:

Abel-Marins-MacBook:a1 abelmarin$ python3 a1\_abelmarin.py

Messege: gjccz, a-1: 1, -b: 0

Messege: hkdda, a-1: 1, -b: 1

Messege: ileeb, a-1: 1, -b: 2

Messege: jmffc, a-1: 1, -b: 3

Messege: knggd, a-1: 1, -b: 4

Messege: lohhe, a-1: 1, -b: 5

Messege: mpiif, a-1: 1, -b: 6

Messege: nqjjg, a-1: 1, -b: 7

Messege: orkkh, a-1: 1, -b: 8

Messege: pslli, a-1: 1, -b: 9

Messege: qtmmj, a-1: 1, -b: 10

Messege: runnk, a-1: 1, -b: 11

Messege: svool, a-1: 1, -b: 12

Messege: twppm, a-1: 1, -b: 13

Messege: uxqqn, a-1: 1, -b: 14

Messege: vyrro, a-1: 1, -b: 15

Messege: wzssp, a-1: 1, -b: 16

Messege: xattq, a-1: 1, -b: 17

Messege: ybuur, a-1: 1, -b: 18

Messege: zcvvs, a-1: 1, -b: 19

Messege: adwwt, a-1: 1, -b: 20

Messege: bexxu, a-1: 1, -b: 21

Messege: cfyyv, a-1: 1, -b: 22

Messege: dgzzw, a-1: 1, -b: 23

Messege: ehaax, a-1: 1, -b: 24

Messege: fibby, a-1: 1, -b: 25

Messege: sbggx, a-1: 3, -b: 0

Messege: vejja, a-1: 3, -b: 1

Messege: yhmmd, a-1: 3, -b: 2

Messege: bkppg, a-1: 3, -b: 3

Messege: enssj, a-1: 3, -b: 4

Messege: hqvvm, a-1: 3, -b: 5

Messege: ktyyp, a-1: 3, -b: 6

Messege: nwbbs, a-1: 3, -b: 7

Messege: qzeev, a-1: 3, -b: 8

Messege: tchhy, a-1: 3, -b: 9

Messege: wfkkb, a-1: 3, -b: 10

Messege: zinne, a-1: 3, -b: 11

Messege: clqqh, a-1: 3, -b: 12

Messege: fottk, a-1: 3, -b: 13

Messege: irwwn, a-1: 3, -b: 14

Messege: luzzq, a-1: 3, -b: 15

Messege: oxcct, a-1: 3, -b: 16

Messege: raffw, a-1: 3, -b: 17

Messege: udiiz, a-1: 3, -b: 18

Messege: xgllc, a-1: 3, -b: 19

Messege: ajoof, a-1: 3, -b: 20

Messege: dmrri, a-1: 3, -b: 21

Messege: gpuul, a-1: 3, -b: 22

Messege: jsxxo, a-1: 3, -b: 23

Messege: mvaar, a-1: 3, -b: 24

Messege: pyddu, a-1: 3, -b: 25

Messege: ykiiw, a-1: 4, -b: 0

Messege: comma, a-1: 4, -b: 1

Messege: gsqqe, a-1: 4, -b: 2

Messege: kwuui, a-1: 4, -b: 3

Messege: oayym, a-1: 4, -b: 4

Messege: seccq, a-1: 4, -b: 5

Messege: wiggu, a-1: 4, -b: 6

Messege: amkky, a-1: 4, -b: 7

Messege: eqooc, a-1: 4, -b: 8

Messege: iussg, a-1: 4, -b: 9

Messege: mywwk, a-1: 4, -b: 10

Messege: qcaao, a-1: 4, -b: 11

Messege: ugees, a-1: 4, -b: 12

Messege: ykiiw, a-1: 4, -b: 13

Messege: comma, a-1: 4, -b: 14

Messege: gsqqe, a-1: 4, -b: 15

Messege: kwuui, a-1: 4, -b: 16

Messege: oayym, a-1: 4, -b: 17

Messege: seccq, a-1: 4, -b: 18

Messege: wiggu, a-1: 4, -b: 19

Messege: amkky, a-1: 4, -b: 20

Messege: eqooc, a-1: 4, -b: 21

Messege: iussg, a-1: 4, -b: 22

Messege: mywwk, a-1: 4, -b: 23

Messege: qcaao, a-1: 4, -b: 24

Messege: ugees, a-1: 4, -b: 25

Messege: qloot, a-1: 7, -b: 0

Messege: xsvva, a-1: 7, -b: 1

Messege: ezcch, a-1: 7, -b: 2

Messege: lgjjo, a-1: 7, -b: 3

Messege: snqqv, a-1: 7, -b: 4

Messege: zuxxc, a-1: 7, -b: 5

Messege: gbeej, a-1: 7, -b: 6

Messege: nillq, a-1: 7, -b: 7

Messege: upssx, a-1: 7, -b: 8

Messege: bwzze, a-1: 7, -b: 9

Messege: idggl, a-1: 7, -b: 10

Messege: pknns, a-1: 7, -b: 11

Messege: wruuz, a-1: 7, -b: 12

Messege: dybbg, a-1: 7, -b: 13

Messege: kfiin, a-1: 7, -b: 14

Messege: rmppu, a-1: 7, -b: 15

Messege: ytwwb, a-1: 7, -b: 16

Messege: faddi, a-1: 7, -b: 17

Messege: mhkkp, a-1: 7, -b: 18

Messege: torrw, a-1: 7, -b: 19

Messege: avyyd, a-1: 7, -b: 20

Messege: hcffk, a-1: 7, -b: 21

Messege: ojmmr, a-1: 7, -b: 22

Messege: vqtty, a-1: 7, -b: 23

Messege: cxaaf, a-1: 7, -b: 24

Messege: jehhm, a-1: 7, -b: 25

Messege: cdssr, a-1: 9, -b: 0

Messege: lmbba, a-1: 9, -b: 1

Messege: uvkkj, a-1: 9, -b: 2

Messege: detts, a-1: 9, -b: 3

Messege: mnccb, a-1: 9, -b: 4

Messege: vwllk, a-1: 9, -b: 5

Messege: efuut, a-1: 9, -b: 6

Messege: noddc, a-1: 9, -b: 7

Messege: wxmml, a-1: 9, -b: 8

Messege: fgvvu, a-1: 9, -b: 9

Messege: opeed, a-1: 9, -b: 10

Messege: xynnm, a-1: 9, -b: 11

Messege: ghwwv, a-1: 9, -b: 12

Messege: pqffe, a-1: 9, -b: 13

Messege: yzoon, a-1: 9, -b: 14

Messege: hixxw, a-1: 9, -b: 15

Messege: qrggf, a-1: 9, -b: 16

Messege: zappo, a-1: 9, -b: 17

Messege: ijyyx, a-1: 9, -b: 18

Messege: rshhg, a-1: 9, -b: 19

Messege: abqqp, a-1: 9, -b: 20

Messege: jkzzy, a-1: 9, -b: 21

Messege: stiih, a-1: 9, -b: 22

Messege: bcrrq, a-1: 9, -b: 23

Messege: klaaz, a-1: 9, -b: 24

Messege: tujji, a-1: 9, -b: 25

Messege: ovwwp, a-1: 11, -b: 0

Messege: zghha, a-1: 11, -b: 1

Messege: krssl, a-1: 11, -b: 2

Messege: vcddw, a-1: 11, -b: 3

Messege: gnooh, a-1: 11, -b: 4

Messege: ryzzs, a-1: 11, -b: 5

Messege: cjkkd, a-1: 11, -b: 6

Messege: nuvvo, a-1: 11, -b: 7

Messege: yfggz, a-1: 11, -b: 8

Messege: jqrrk, a-1: 11, -b: 9

Messege: ubccv, a-1: 11, -b: 10

Messege: fmnng, a-1: 11, -b: 11

Messege: qxyyr, a-1: 11, -b: 12

Messege: bijjc, a-1: 11, -b: 13

Messege: mtuun, a-1: 11, -b: 14

Messege: xeffy, a-1: 11, -b: 15

Messege: ipqqj, a-1: 11, -b: 16

Messege: tabbu, a-1: 11, -b: 17

Messege: elmmf, a-1: 11, -b: 18

Messege: pwxxq, a-1: 11, -b: 19

Messege: ahiib, a-1: 11, -b: 20

Messege: lsttm, a-1: 11, -b: 21

Messege: wdeex, a-1: 11, -b: 22

Messege: hoppi, a-1: 11, -b: 23

Messege: szaat, a-1: 11, -b: 24

Messege: dklle, a-1: 11, -b: 25

Messege: mfeel, a-1: 15, -b: 0

Messege: butta, a-1: 15, -b: 1

Messege: qjiip, a-1: 15, -b: 2

Messege: fyxxe, a-1: 15, -b: 3

Messege: unmmt, a-1: 15, -b: 4

Messege: jcbbi, a-1: 15, -b: 5

Messege: yrqqx, a-1: 15, -b: 6

Messege: ngffm, a-1: 15, -b: 7

Messege: cvuub, a-1: 15, -b: 8

Messege: rkjjq, a-1: 15, -b: 9

Messege: gzyyf, a-1: 15, -b: 10

Messege: vonnu, a-1: 15, -b: 11

Messege: kdccj, a-1: 15, -b: 12

Messege: zsrry, a-1: 15, -b: 13

Messege: ohggn, a-1: 15, -b: 14

Messege: dwvvc, a-1: 15, -b: 15

Messege: slkkr, a-1: 15, -b: 16

Messege: hazzg, a-1: 15, -b: 17

Messege: wpoov, a-1: 15, -b: 18

Messege: leddk, a-1: 15, -b: 19

Messege: atssz, a-1: 15, -b: 20

Messege: pihho, a-1: 15, -b: 21

Messege: exwwd, a-1: 15, -b: 22

Messege: tmlls, a-1: 15, -b: 23

Messege: ibaah, a-1: 15, -b: 24

Messege: xqppw, a-1: 15, -b: 25

Messege: yxiij, a-1: 17, -b: 0

Messege: pozza, a-1: 17, -b: 1

Messege: gfqqr, a-1: 17, -b: 2

Messege: xwhhi, a-1: 17, -b: 3

Messege: onyyz, a-1: 17, -b: 4

Messege: feppq, a-1: 17, -b: 5

Messege: wvggh, a-1: 17, -b: 6

Messege: nmxxy, a-1: 17, -b: 7

Messege: edoop, a-1: 17, -b: 8

Messege: vuffg, a-1: 17, -b: 9

Messege: mlwwx, a-1: 17, -b: 10

Messege: dcnno, a-1: 17, -b: 11

Messege: uteef, a-1: 17, -b: 12

Messege: lkvvw, a-1: 17, -b: 13

Messege: cbmmn, a-1: 17, -b: 14

Messege: tsdde, a-1: 17, -b: 15

Messege: kjuuv, a-1: 17, -b: 16

Messege: ballm, a-1: 17, -b: 17

Messege: srccd, a-1: 17, -b: 18

Messege: jittu, a-1: 17, -b: 19

Messege: azkkl, a-1: 17, -b: 20

Messege: rqbbc, a-1: 17, -b: 21

Messege: ihsst, a-1: 17, -b: 22

Messege: zyjjk, a-1: 17, -b: 23

Messege: qpaab, a-1: 17, -b: 24

Messege: hgrrs, a-1: 17, -b: 25

Messege: kpmmh, a-1: 19, -b: 0

Messege: diffa, a-1: 19, -b: 1

Messege: wbyyt, a-1: 19, -b: 2

Messege: purrm, a-1: 19, -b: 3

Messege: inkkf, a-1: 19, -b: 4

Messege: bgddy, a-1: 19, -b: 5

Messege: uzwwr, a-1: 19, -b: 6

Messege: nsppk, a-1: 19, -b: 7

Messege: gliid, a-1: 19, -b: 8

Messege: zebbw, a-1: 19, -b: 9

Messege: sxuup, a-1: 19, -b: 10

Messege: lqnni, a-1: 19, -b: 11

Messege: ejggb, a-1: 19, -b: 12

Messege: xczzu, a-1: 19, -b: 13

Messege: qvssn, a-1: 19, -b: 14

Messege: jollg, a-1: 19, -b: 15

Messege: cheez, a-1: 19, -b: 16

Messege: vaxxs, a-1: 19, -b: 17

Messege: otqql, a-1: 19, -b: 18

Messege: hmjje, a-1: 19, -b: 19

Messege: afccx, a-1: 19, -b: 20

Messege: tyvvq, a-1: 19, -b: 21

Messege: mrooj, a-1: 19, -b: 22

Messege: fkhhc, a-1: 19, -b: 23

Messege: ydaav, a-1: 19, -b: 24

Messege: rwtto, a-1: 19, -b: 25

Messege: whqqf, a-1: 21, -b: 0

Messege: rclla, a-1: 21, -b: 1

Messege: mxggv, a-1: 21, -b: 2

Messege: hsbbq, a-1: 21, -b: 3

Messege: cnwwl, a-1: 21, -b: 4

Messege: xirrg, a-1: 21, -b: 5

Messege: sdmmb, a-1: 21, -b: 6

Messege: nyhhw, a-1: 21, -b: 7

Messege: itccr, a-1: 21, -b: 8

Messege: doxxm, a-1: 21, -b: 9

Messege: yjssh, a-1: 21, -b: 10

Messege: tennc, a-1: 21, -b: 11

Messege: oziix, a-1: 21, -b: 12

Messege: judds, a-1: 21, -b: 13

Messege: epyyn, a-1: 21, -b: 14

Messege: zktti, a-1: 21, -b: 15

Messege: ufood, a-1: 21, -b: 16

Messege: pajjy, a-1: 21, -b: 17

Messege: kveet, a-1: 21, -b: 18

Messege: fqzzo, a-1: 21, -b: 19

Messege: aluuj, a-1: 21, -b: 20

Messege: vgppe, a-1: 21, -b: 21

Messege: qbkkz, a-1: 21, -b: 22

Messege: lwffu, a-1: 21, -b: 23

Messege: graap, a-1: 21, -b: 24

Messege: bmvvk, a-1: 21, -b: 25

Messege: izuud, a-1: 23, -b: 0

Messege: fwrra, a-1: 23, -b: 1

Messege: ctoox, a-1: 23, -b: 2

Messege: zqllu, a-1: 23, -b: 3

Messege: wniir, a-1: 23, -b: 4

Messege: tkffo, a-1: 23, -b: 5

Messege: qhccl, a-1: 23, -b: 6

Messege: nezzi, a-1: 23, -b: 7

Messege: kbwwf, a-1: 23, -b: 8

Messege: hyttc, a-1: 23, -b: 9

Messege: evqqz, a-1: 23, -b: 10

Messege: bsnnw, a-1: 23, -b: 11

Messege: ypkkt, a-1: 23, -b: 12

Messege: vmhhq, a-1: 23, -b: 13

Messege: sjeen, a-1: 23, -b: 14

Messege: pgbbk, a-1: 23, -b: 15

Messege: mdyyh, a-1: 23, -b: 16

Messege: javve, a-1: 23, -b: 17

Messege: gxssb, a-1: 23, -b: 18

Messege: duppy, a-1: 23, -b: 19

Messege: armmv, a-1: 23, -b: 20

Messege: xojjs, a-1: 23, -b: 21

Messege: ulggp, a-1: 23, -b: 22

Messege: riddm, a-1: 23, -b: 23

Messege: ofaaj, a-1: 23, -b: 24

Messege: lcxxg, a-1: 23, -b: 25

Messege: uryyb, a-1: 25, -b: 0

Messege: tqxxa, a-1: 25, -b: 1

Messege: spwwz, a-1: 25, -b: 2

Messege: rovvy, a-1: 25, -b: 3

Messege: qnuux, a-1: 25, -b: 4

Messege: pmttw, a-1: 25, -b: 5

Messege: olssv, a-1: 25, -b: 6

Messege: nkrru, a-1: 25, -b: 7

Messege: mjqqt, a-1: 25, -b: 8

Messege: lipps, a-1: 25, -b: 9

Messege: khoor, a-1: 25, -b: 10

Messege: jgnnq, a-1: 25, -b: 11

Messege: ifmmp, a-1: 25, -b: 12

Messege: hello, a-1: 25, -b: 13

Messege: gdkkn, a-1: 25, -b: 14

Messege: fcjjm, a-1: 25, -b: 15

Messege: ebiil, a-1: 25, -b: 16

Messege: dahhk, a-1: 25, -b: 17

Messege: czggj, a-1: 25, -b: 18

Messege: byffi, a-1: 25, -b: 19

Messege: axeeh, a-1: 25, -b: 20

Messege: zwddg, a-1: 25, -b: 21

Messege: yvccf, a-1: 25, -b: 22

Messege: xubbe, a-1: 25, -b: 23

Messege: wtaad, a-1: 25, -b: 24

Messege: vszzc, a-1: 25, -b: 25