Vivek Patel

CSC 440

Assignment 1

1. 1. vortex = 21, 14, 17, 19, 4, 23 Function is (19x + 12)mod 26

Pre-mod: 411, 278, 335, 373, 88, 449

Post-mod: 21, 18, 23, 9, 10, 7

Ciphertext: VSXJKH

* 1. y = 19x + 12

x = (y – 12)/19

x = 11(y – 12)

x = 11y – 132

x = 11y + 24

decryption function: (11x + 24)mod26

1. HCNKR = 7, 2, 13, 10, 17

y = 5x + 10

x = (y – 10)/5

x = 21y – 210

x = 21y + 24 (decryption function)

Pre-mod: 171, 66, 297, 234, 381

Post-mod: 15, 14, 11, 0, 17

Plaintext: POLAR

1. gcd(a, 33) = 1 is at 20 (1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20, 23, 25, 26, 28, 29, 31, 32)

20 \* 33 = 660 keys for the Gregorian Alphabet

1. gcd(a, 31) = 1 is 30 (31 is a prime number)

30 \* 31 = 930 keys

1. with a shift of 2, the ciphertext is decrypted as “watchoutforbrutus”, or “watch out for brutus”
2. 1. TCCAAGTGTTGGTGCCAACCGGGAGCGACCCTTTCAGAGACTCCGA
   2. Program included in zip file labeled as “Question6b.java”

Some restrictions on the affine cipher are the limited number of options for “a” and “b” in the formula f(x) = ax + b due to the small size of the alphabet used. “a” can only use 1 and 3 to fulfill the gcd(a, 4) = 1 requirement and b only has 4 options leaving us with a keyspace of 8.

1. Program included in zip file labeled as “Question7.java”

Output:

shift = 1, confidence = 16

shift = 2, confidence = 7

shift = 3, confidence = 16

shift = 4, confidence = 22

shift = 5, confidence = 14

shift = 6, confidence = 15

shift = 7, confidence = 40

shift = 8, confidence = 14

shift = 9, confidence = 11

shift = 10, confidence = 12

shift = 11, confidence = 18

shift = 12, confidence = 18

shift = 13, confidence = 11

shift = 14, confidence = 27

1. And yet, even though cryptography has influenced human affairs for millenia, developments over the last thirty years have completely, yes completely, changed our understanding of it. If you plotted when the basic mathematical discoveries in cryptography were made you would see a few in antiquity, maybe a few from the middle ages till the eighteen hundreds, one in the nineteen twenties, the one time pad a few more around World War Two, and then after the birth of computational complexity theory in the nineteen seventies. boomboomboomboomboomboomboomx

Tool used: <https://planetcalc.com/7956/>

Decrypted text, untouched:

andyeteventhoughcryptographyhasinfluencedhumanaffairsformilleniadevelopmentsoverthelastthirtyyearshavecompletelyyescompletelychangedourunderstandingofitifyouplottedwhenthebasicmathematicaldiscoveriesincryptographyweremadeyouwouldseeafewinantiquitymaybeafewfromthemiddleagestilltheeighteenhundredsoneinthenineteentwentiestheonetimepadafewmorearoundworldwartwoandthenafterthebirthofcomputationalcomplexitytheoryinthenineteenseventiesboomboomboomboomboomboomboomx