Cryptography Midterm

1. (After Guessing and Checking Using Program)

Shift = 18

BELINDA CUT THE BIG CHEESE ON THE BUS FROM MINNESOTA AND WE WERE FORCED TO BREATHE IT ALL THE WAY TO SOUTH DAKOTA THIS SILENT DEADLY STINK BOMB TOOK ITS TOLL ON ALL OF US SOON TWENTY KIDS WERE PUKING OUT THE WINDOWS OF THE BUS THAT ROTTEN EGG JUST LINGERED THE WHOLE WAY TO MOUNT RUSHMORE BELINDA CUT A BIG SLICE OF A CHEESE LIKE NONE BEFORE

1. BELIN DA 🡪 WDCVY SL

|  |  |
| --- | --- |
| X | E(x) |
| 1 | 22 |
| 4 | 3 |
| 11 | 2 |
| 8 | 21 |
| 13 | 24 |
| 3 | 18 |
| 0 | 11 |

(After Guessing and Checking using Calculator)

E(x) = (11x + 11) % 26

D(y) = (19x + 25) % 26

BELINDA ATE A BOOGER ON OUR FIELD TRIP TO KENTUCKY I CANT BELIEVE SHE DID THAT ITS JUST SO VERY YUCKY I THINK ITS REALLY NASTY ID DIE IF THEY ALL KNEW ONE TIME IN THE FIRST GRADE I ATE A BOOGER TOO

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | X | Y | Z |
| 17 | 29 | 8 | 12 | 20 | 21 | 12 | 2 | 7 | 2 | 5 | 1 | 20 | 2 | 7 | 7 | 23 | 1 | 6 | 12 | 13 | 5 | 10 | 8 |
| 6.773 | 11.554 | 3.187 | 4.781 | 7.968 | 8.367 | 4.781 | .797 | 2.789 | .797 | 1.992 | .398 | 7.968 | .797 | 2.789 | 2.789 | 9.163 | .398 | 2.390 | 4.781 | 5.179 | 1.992 | 3.984 | 3.187 |

1. Trust Spaces to Mean Different Words

251 Letters

A🡪N; B🡪O; C🡪 P; D🡪Q; E🡪R; F🡪S; G🡪 T

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

Encryption Shift of 13

DO NOT TASTE THE EARWAX! HEAR ME OUT! I'M KEEPING TABS! NEVER PLAY WITH MUCUS! NEVER LICK THE OOZING SCABS! DO NOT POP THE PIMPLES, AS YOU KNEEL AT MORNING MASS! DO NOT SWALLOW LOOGIES, SHOULD YOU COUGH ONE UP IN CLASS! THIS IS YOUR LAST WARNING... SO NO MATTER WHAT YOU DO... DO NOT TASTE THE EARWAX... OR DRINK UPCHUCK FROM A SHOE!

***6.*** (I’ll do the Example for A Keyword Length of 4, 5 and 6 w/ My Own Program)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  |  |  |  | | --- | --- | --- | --- | | Keyword Length 4 Frequencies | Keyword Length 5 Frequencies | Keyword Length 6 Frequencies | Signature of Printed English | |  |  |  |  | | A: 0.049999999999999996 | A: 0.05 | A: 0.05026455026455026 | A: 0.08167 | | B: 0.021052631578947368 | B: 0.021052631578947368 | B: 0.021164021164021163 | B: 0.01492 | | C: 0.0368421052631579 | C: 0.036842105263157884 | C: 0.037037037037037035 | C: 0.02782 | | D: 0.049999999999999996 | D: 0.05 | D: 0.05026455026455026 | D: 0.04253 | | E: 0.0368421052631579 | E: 0.0368421052631579 | E: 0.037037037037037035 | E: 0.12702 | | F: 0.03421052631578947 | F: 0.03421052631578947 | F: 0.03439153439153439 | F: 0.02228 | | G: 0.05526315789473684 | G: 0.055263157894736833 | G: 0.05555555555555555 | G: 0.02015 | | H: 0.031578947368421054 | H: 0.031578947368421054 | H: 0.031746031746031744 | H: 0.06094 | | I: 0.07631578947368421 | I: 0.07631578947368421 | I: 0.07671957671957672 | I: 0.06966 | | J: 0.034210526315789476 | J: 0.034210526315789476 | J: 0.03439153439153439 | J: 0.00153 | | K: 0.039473684210526314 | K: 0.039473684210526314 | K: 0.03968253968253968 | K: 0.00772 | | L: 0.0368421052631579 | L: 0.0368421052631579 | L: 0.037037037037037035 | L: 0.04025 | | M: 0.05526315789473685 | M: 0.05526315789473685 | M: 0.05555555555555555 | M: 0.02406 | | N: 0.013157894736842105 | N: 0.013157894736842105 | N: 0.013227513227513227 | N: 0.06749 | | O: 0.007894736842105263 | O: 0.007894736842105263 | O: 0.007936507936507936 | O: 0.07507 | | P: 0.047368421052631574 | P: 0.047368421052631574 | P: 0.047619047619047616 | P: 0.01929 | | Q: 0.015789473684210527 | Q: 0.015789473684210527 | Q: 0.015873015873015872 | Q: 0.00095 | | R: 0.023684210526315787 | R: 0.023684210526315787 | R: 0.023809523809523808 | R: 0.05987 | | S: 0.06315789473684211 | S: 0.06315789473684211 | S: 0.06349206349206349 | S: 0.06327 | | T: 0.03421052631578947 | T: 0.03421052631578947 | T: 0.03439153439153439 | T: 0.09056 | | U: 0.018421052631578946 | U: 0.018421052631578946 | U: 0.018518518518518517 | U: 0.02758 | | V: 0.023684210526315787 | V: 0.023684210526315787 | V: 0.023809523809523808 | V: 0.00978 | | W: 0.07894736842105263 | W: 0.07894736842105263 | W: 0.07936507936507936 | W: 0.02360 | | X: 0.034210526315789476 | X: 0.034210526315789476 | X: 0.03439153439153439 | X: 0.00150 | | Y: 0.02631578947368421 | Y: 0.02631578947368421 | Y: 0.026455026455026454 | Y: 0.01974 | | Z: 0.04736842105263158 | Z: 0.04736842105263158 | Z: 0.047619047619047616 | Z: 0.00074 | |  |  |

Keyword Length = 5

***7.*** Keyword: PILES

HAVE YOU SEEN MY POOPASAURUS OH SHE POOPS IN GREAT BIG PILES SHES A PREHISTORIC CREAT URE AND HER POOP GOES ON FOR MILES CAN YOU HELP ME TO LOCATE HER THOUGH YOUR NOSE WONT LIKE IT MUCH IF YOU SEE HER PLEASE REMEMBER YOU CAN LOOK BUT DO NOT TOUCH DO NOT TOUCH MY POOPASAURUS OR SHE MAY JUST POOP ON YOU SHE ESCAPED ME JUST THIS MORNING WHEN I TOOK HER OUT TO POO HAVE YOU SEEN MY POOPASAURUS SHES THE ONLY PET IVE GOT SHES CUTE AND KIND BUT KEEP IN MIND SHE POOPS AN AWFUL LOT

***8.*** (Using My Own Personal Hill Cipher Program)

IF YOU THINK THAT BOOGER WAS GROSS BE GLAD YOU MISSED THE COUNTY FAIR BELINDA PUKED ON ALL THE RIDES AND HER SLIME GOT IN MY HAIR WHILE TWIRLING ON THE LOOP D LOOP I LOOKED UP TOWARD THE SKY I SAW BELINDA HIGH ABOVE AND HER BARF FELL IN MY EYE BELINDA STARTED BLOWING CHUNKS ALL OVER MY LITTLE SISTER SHE SPEWED SOME ON THE TILT A WHIRL SHE SPEWED SOME ON THE TWISTER WE SAW A MOST UNSIGHTLY GREEN AS BELINDA RODE THE COMET WHILE SHE HOVERED WE GOT COVERED IN ICKY STICKY PICKLE VOMIT

***9.*** ECB: Simplest one. Divides message into blocks and encrypts them separately. However, doesn’t hide data patterns well.

CBC: Message is divided into blocks. Each block is exclusive-or’ed with block of cipher text before it, before being encrypted as well. Thus, each cipher text block is dependent on all plaintext blocks before it.

CFB: Makes block cipher into stream cipher (encrypt bits as you go) that is self- synchronizing. Very close to CBC. For example, CFB decryption is almost identical to CBC encryption done in reverse.