NCSSM Summer Accelerator Cryptography and Cryptanalysis

# Cracking the Vigenere Cipher

Suppose we had the following piece of a plaintext message:

… on a plane. The plane is due…

Even though the word plane appears twice in the message, we know that if we use a polyalphabetic substitution cipher, like the Vigenere Cipher, there’s no guarantee that it will be encrypted the same way both times. However, maybe it will some of the time?

Use the keyword “water” to encrypt the message:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Keyword | *w* | *a* | *t* | *e* | *r* | *w* | *a* | *t* | *e* | *r* | *w* | *a* | *t* | *e* | *r* | *w* | *a* | *t* | *e* | *r* | *w* |
| Plaintext | o | n | a | p | l | a | n | e | t | h | e | p | l | a | n | e | i | s | d | u | e |
| Ciphertext |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Now use the keyword “milk”

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Keyword | *m* | *i* | *l* | *k* | *m* | *i* | *l* | *k* | *m* | *i* | *l* | *k* | *m* | *i* | *l* | *k* | *m* | *i* | *l* | *k* | *m* |
| Plaintext | o | n | a | p | l | a | n | e | t | h | e | p | l | a | n | e | i | s | d | u | e |
| Ciphertext |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Now use the keyword “hospital”

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Keyword | *h* | *o* | *s* | *p* | *i* | *t* | *a* | *l* | *h* | *o* | *s* | *p* | *i* | *t* | *a* | *l* | *h* | *o* | *s* | *p* | *i* |
| Plaintext | o | n | a | p | l | a | n | e | t | h | e | p | l | a | n | e | i | s | d | u | e |
| Ciphertext |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

What is it about some of the keywords that results in the word plane being encrypted into the same ciphertext? What are possible lengths of keywords that will cause this to happen?

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *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* |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Suppose we had the following ciphertext that we suspect was encrypted using a Vigenere cipher:

000 JAKXQ SWECW MMJBK TQMCM LWCXJ BNEWS XKRBO IAOBI 040 NOMLJ GUIMH YTACF ICVOE BGOVC WYRCV KXJZV SMRXY 080 VPOVB UBIJH OVCVK RXBOE ASZVR AOXQS WECVO QJHSG 120 ROXWJ MCXQF OIRGZ VRAOJ RJOMB DBMVS CIESX MBDBM 160 VSKRM GYFHA KXQSW ECWME UWXHD QDMXB KPUCN HWIWF 200 NFCKA SKXNF DLJBY RNOBI YFSQN HRIYV IWRQS WCGKC 240 BHRVN SSWYF SQNTS ZNWCT AWWIB SFIWW CTAWW IWWXI 280 RGKRN LZIAW WIWHK PNFBS ASVIE SXMBD BMVSK RMGYC 320 NGKPU CNHWI WFNFC KASKX NFDLJ BYRNO BIYFS QNHRI 360 NBQMW SOVBO IWCVB INWCT AWWIO WFIRG ZVRAO WNJOR 400 RGZVR AORRB OMBDB MVSOP NJORR GZVRA OXQWB XNSXM 440 BDBMV SPMOH OIWWC TAWWI

|  |  |  |  |
| --- | --- | --- | --- |
| **Repeated String** | **Position of first letter in the string** | **Distance between pairs of occurrences of the string** | **Prime factorization of the distance between pairs of occurrences of the string** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Guess for the length of the keyword: