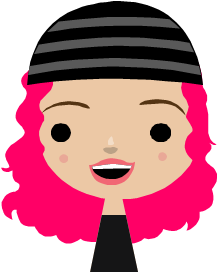
Interlock Rochester Presents:

How Do I ... Crypto Workbook

Author: NAGVGERR

Statistical Analysis of Substitution Ciphers:

Interlock Rochester is the only place in Rochester that can teach you crypto! Isn’t that cool?

Kgsrpdhtb Phtcrqsrp kq scr hgdy jditr kg Phtcrqsrp scis tig sritc yhu

tpyjsh! Kqg’s scis thhd?

YOU MAY HAVE EXPECTED THIS PARAGRAPH TO START WITH INTERLOCK

AIC KZA RZPV VLHVXDVW DRQE HZFZTFZHR DI EDZFD SQDR QJDVFMIXN

BUT I THOUGHT THAT WOULD BE TOO OBVIOUS INSTEAD I AM SHOWING

YCD Q DRICTRD DRZD SICMW YV DII IYPQICE QJEDVZW Q ZK ERISQJT

YOU THIS PARAGRAPH THAT CONTAINS A LOT OF WORDS TO MAKE IT MORE

AIC DRQE HZFZTFZHR DRZD XIJDZQJE Z MID IU SIFWE DI KZNV QD KIFV

LIKELY THAT YOULL BE ABLE TO DEDUCE WHAT THE CIPHER MAY BE

MQNVMA DRZD AICMM YV ZYMV DI WVWCXV SRZD DRV XQHRVF KZA YV

GETTINGHARDYET?IBETITIS.SEEHOWTHELESSCLUESYOUGETTHEHARDERITBECOMES?

QSFFMDQOYBTZSF?MXSFMFMH.HSSOCPFOSGSHHVGJSHZCJQSFFOSOYBTSBMFXSVCESH?

ENCRYPTING OR ENCODING

454E4352595054494E47204F5220454E434F44494E47

One time Pads

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

47 42 82 55 53 46 33 06 40 21 71 47 28 34 07 25 01 76 63 91 93 83 68 36 38 35 67 52 10 30 12 49 51 85 27 75 37 60 70 99

53974 37661 62247 51515 55215 78278 23120 66822 08432 28479 93515 09337 16038 10492 79023 35173 17668 27860 58662 57206

47650 99517 83450 37714 87253 40161 71947 94646 33989 91772 16041 38245 32727 42217 85083 08475 78183 31256 88951 70392

08716 11468 04722 15330 01907 07747 95576 19865 76959 16459 56156 85450 15563 28214 88174 09054 00015 79115 12179 40771

15023 43248 74886 45557 17925 97664 78071 31466 33121 76632 34036 53310 89887 02948 58170 34608 83397 04146 12691 39324

28245 37097 88117 92206 91851 98130 55889 32641 42054 84604 29614 71384 34023 96560 70385 86057 58719 29057 59251 65822

80328 90595 24496 32547 39655 82165 35567 45895 41081 61416 14680 26233 77834 67046 59857 01942 55724 74197 47531 90895

55430 13208 46428 89399 14768 85865 31085 19930 78710 69999 80356 14200 84282 79173 24195 15514 40586 20040 13441 72199

41360 88630 18066 68673 78622 89408 35961 05069 08704 37304 77239 52893 63860 07514 41222 66906 47371 32312 78555 56217

66988 15416 06343 47589 85831 49860 53652 57798 30575 81340 32626 76563 51627 87467 30888 46071 01363 94040 30293 98035

86675 41148 34961 36631 66196 48552 04971 41265 19006 24287 35454 10366 57054 10547 15726 34062 80725 13649 20736 14679

39411 04511 89151 77541 56229 84452 39180 28580 66981 16870 02735 72917 15633 75224 29027 24311 42315 88880 50523 99922

35147 86227 36978 56634 68521 81183 41955 74197 92489 24587 05657 74992 33429 99318 01149 07465 17173 85784 01843 73305

11626 63300 91809 19497 99873 24755 27799 45376 47828 74713 50248 66232 86955 99137 87560 33415 77691 56879 06502 19233

91057 09140 72842 99877 78338 54878 27923 73288 36110 31019 79712 67755 57350 62381 21833 86498 37718 07683 14049 11250

47221 51890 73754 65224 54969 87012 05027 17897 97162 52775 22918 80681 89781 50930 72789 94271 79461 35194 38306 56659

62241 13540 71918 04424 85216 97262 23557 77021 00301 11653 14936 63399 61226 99392 50280 40205 52056 61990 86218 90730

08126 26747 20925 69758 84405 30603 70283 90065 89582 14189 07348 98858 12931 32138 71739 94413 31076 86471 38432 56579

44127 12253 59467 05342 58191 45792 73795 51877 13650 36671 93903 05875 15884 43521 24499 53611 70461 77654 17006 45908

13262 21683 76312 48914 42253 80880 79496 72730 00642 99190 64389 66954 92442 01584 59523 72281 24563 42938 43197 49898

35788 06035 26082 32536 47056 89679 41410 22636 15223 45608 34649 32990 84136 16889 59572 82752 69623 65655 64988 59447

<http://goo.gl/3rzEAN>

1) DYHFIQBJ-KUMLWDFE-LXNSXBMN-FERYPNIK-HKLIIFVX-OQXXCDAX-LHPVDXXP-PFYXNVXU

2) BJENFSOX-HVNKYPZV-FWPYCBIF-ADSWEFVQ-IRNVSMDK-AZLBRLSK-RHUIBSVG-RNMIDEJV

3) CBQJYPAP-MFLQAFSI-DJVQCRZF-LYNIZHOI-QMKNUYET-MEFKSHLV-PXQMGDLP-ZZCOYIEG

4) OXOJHAKI-EYIEKCWH-VCUOGYMH-CZVYATHQ-HMZNZDIL-AJVHBYPK-LULFZWFR-LTPWXLNL

5) TFSSASNO-XRBUBGIS-IZHNZPQF-HKVELWNG-OHKWGAKF-MQXVQEMY-TXHQHOHN-KAKEXBLP

6) MYCTYAVD-DBKINJKP-VIVOLFIG-DCULYMDT-HJLJGZWF-NSHJLDAJ-REFHATRJ-XZQBFRGW

7) PPEHUFWE-JDHPGGNB-QNLHRMRK-RDTLTFJU-NLMTVDQN-WBFWCQZB-BBYMKKPE-HMPBCERF

8) BGWVAIDJ-MSPCNGJA-UGGXDFKW-DXRHGZOQ-EUCFMNUB-XBYOTDUH-AQGXUESA-LNTPTYLG

9) WBIXKEZO-BLWGJCGL-HQIPQRSE-JODVVKUX-XUHSWEIL-FJYGUIDD-MJRWRMWU-EGNEBUSZ

10) FUYNHHYY-KKOCJELL-KUHOKNHC-GDVQUQPS-KINNAQQA-HMJFUZGE-KJFLFVAY-MYWUTTNO

Plaintext to encode: HELLO FRIEND

Post Verification

Greg has developed a web application that logs into Interlock’s website. Answer the questions based on this POST request that you’ve intercepted:

POST http://www.interlockroc.org/login.php HTTP/1.1

User-Agent: Interlock Explorer v12.0

Referrer: https://www.antitree.com

Content-Length: 99

Host: interlockroc.org

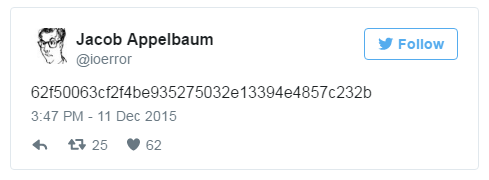
username=antitree&password=supersecurepassword&csrf=TEST&verification= 5F6BEBA5B0E1DC8E4126D48E02FF45F493614D071776552EB01EE4F5D8906E03FEBA3EE8C5A3E0EE5C68FD77217A7FAC949066AE883EF755312B5715DDC7EA5F

1. What kind of hash is the verification value?
2. Why do you think someone would try to hash the body of request?
3. Are there any benefits to this?
4. Are there any reasons this is a bad idea?

Hashtag Hash

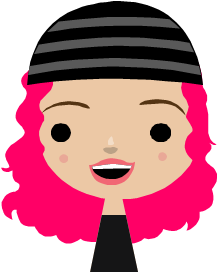
Do you think this is a hash, cipher, or encoding?

Why would someone do this on Twitter?



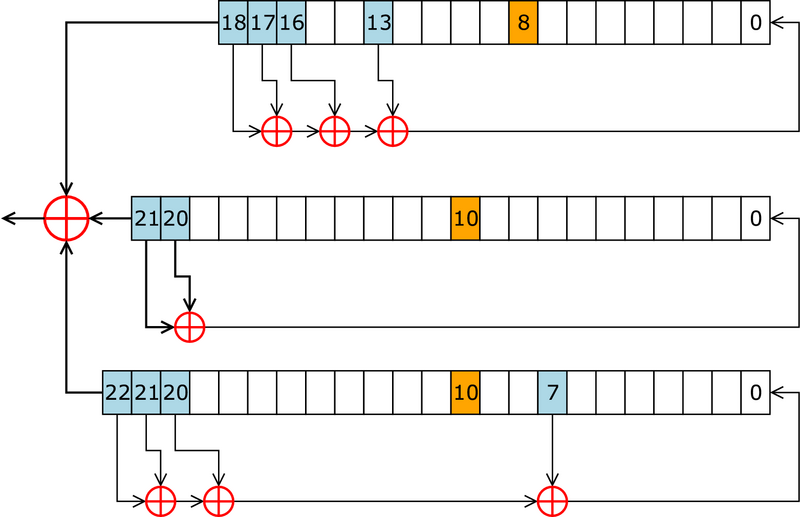
Applied Crypto

The zombie apocalypse has happened except that the zombies are resourceful, nation-state adversaries able to intercept your communications in order to track, target, and eventually eat your brains. You need to give your friends a secret message that is sent over the Internet. By the way, the only website that works is zombie owned social networking site:BrainBook.com. Design a cryptographic protocol that will be able to facilitate communications without the zombies being able to crack it.

Block and Stream Ciphers

A5-1 Stream Cipher



Block Cipher

