School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

CYBR 171 T1 2023

Ngā whakapūtanga o Te Haumaru rorohiko

Cybersecurity Fundamentals

Frequency Analysis

Useful Links

- Caesar Cipher
  - https://cryptii.com/pipes/caesar-cipher
- Vigenere Cipher:
  - CSFG: https://cryptii.com/pipes/vigenere-cipher
  - Decode: https://www.dcode.fr/vigenere-cipher
- Frequency counter:
  - http://users.bestweb.net/~quenell/s2003/ma139/js/count.html
- Letter frequency:
  - https://en.wikipedia.org/wiki/Letter_frequency
- Letter frequency
  - https://studio.code.org/s/frequency_analysis/lessons/1/levels/1

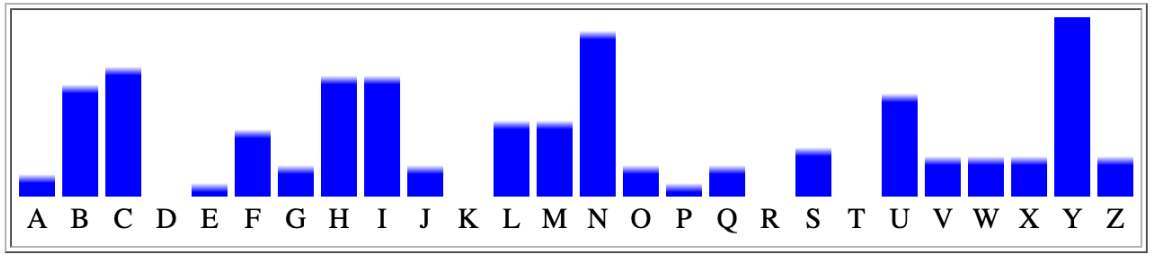
PART I:
Caesar Cipher

Caesar Cipher–Example 1

C HYYX MUS HINBCHA BYLY, IH NBY ZCLMN BYUX, VYWUOMY HINBCHA WUH MBIQ VYNNYL NBUH GS BCMNILS QBYNBYL NBUN JLYXCWNCIH QUM PYLCZCYX IL ZUFMCZCYX VS NBY LYMOFN. IH NBY MYWIHX VLUHWB IZ NBY KOYMNCIH, C QCFF IHFS LYGULE, NBUN OHFYMM C LUH NBLIOAB NBUN JULN IZ GS CHBYLCNUHWY QBCFY C QUM MNCFF U VUVS, C BUPY HIN WIGY CHNI CN SYN. VON C XI HIN UN UFF WIGJFUCH IZ BUPCHA VYYH EYJN ION IZ NBCM JLIJYLNS; UHX CZ UHSVIXS YFMY MBIOFX VY CH NBY JLYMYHN YHDISGYHN IZ CN, BY CM BYULNCFS QYFWIGY NI EYYJ CN.

Caesar 1—Analysis

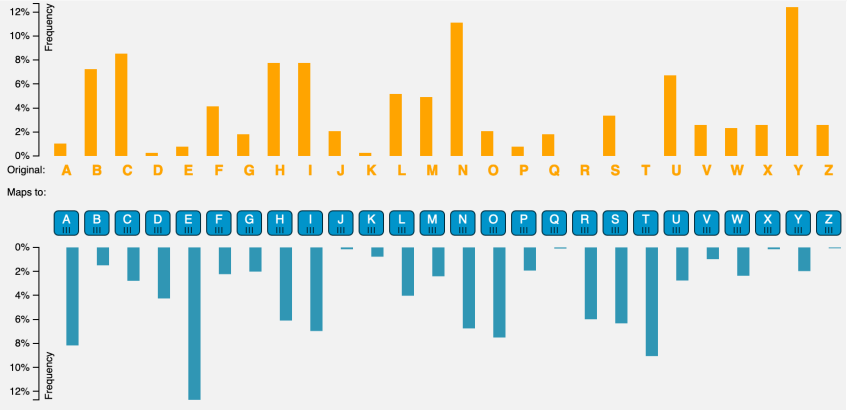
- C HYYX MUS HINBCHA BYLY, IH NBY ZCLMN BYUX, VYWUOMY HINBCHA WUH MBIQ VYNNYL NBUH GS BCMNILS QBYNBYL NBUN JLYXCWNCIH QUM PYLCZCYX IL ZUFMCZCYX VS NBY LYMOFN. IH NBY MYWIHX VLUHWB IZ NBY KOYMNCIH, C QCFF IHFS LYGULE, NBUN OHFYMM C LUH NBLIOAB NBUN JULN IZ GS CHBYLCNUHWY QBCFY C QUM MNCFF U VUVS, C BUPY HIN WIGY CHNI CN SYN. VON C XI HIN UN UFF WIGJFUCH IZ BUPCHA VYYH EYJN ION IZ NBCM JLIJYLNS; UHX CZ UHSVIXS YFMY MBIOFX VY CH NBY JLYMYHN YHDISGYHN IZ CN, BY CM BYULNCFS QYFWIGY NI EYYJ CN.



- 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
- U V W X **Y** Z A B C D E F G H I J K L M N O P Q R S T
- Encrypt shift right 20
- Decrypt shift left 20
- I NEED SAY NOTHING HERE, ON THE FIRST HEAD, BECAUSE NOTHING CAN SHOW BETTER THAN MY HISTORY WHETHER THAT PREDICTION WAS VERIFIED OR FALSIFIED BY THE RESULT. ON THE SECOND BRANCH OF THE QUESTION, I WILL ONLY REMARK, THAT UNLESS I RAN THROUGH THAT PART OF MY INHERITANCE WHILE I WAS STILL A BABY, I HAVE NOT COME INTO IT YET. BUT I DO NOT AT ALL COMPLAIN OF HAVING BEEN KEPT OUT OF THIS PROPERTY; AND IF ANYBODY ELSE SHOULD BE IN THE PRESENT ENJOYMENT OF IT, HE IS HEARTILY WELCOME TO KEEP IT.

Caesar 1—Analysis (cont.)

C HYYX MUS HINBCHA BYLY, IH NBY ZCLMN BYUX, VYWUOMY HINBCHA WUH MBIQ VYNNYL NBUH GS BCMNILS QBYNBYL NBUN JLYXCWNCIH QUM PYLCZCYX IL ZUFMCZCYX VS NBY LYMOFN. IH NBY MYWIHX VLUHWB IZ NBY KOYMNCIH, C QCFF IHFS LYGULE, NBUN OHFYMM C LUH NBLIOAB NBUN JULN IZ GS CHBYLCNUHWY QBCFY C QUM MNCFF U VUVS, C BUPY HIN WIGY CHNI CN SYN. VON C XI HIN UN UFF WIGJFUCH IZ BUPCHA VYYH EYJN ION IZ NBCM JLIJYLNS; UHX CZ UHSVIXS YFMY MBIOFX VY CH NBY JLYMYHN YHDISGYHN IZ CN, BY CM BYULNCFS QYFWIGY NI EYYJ CN.



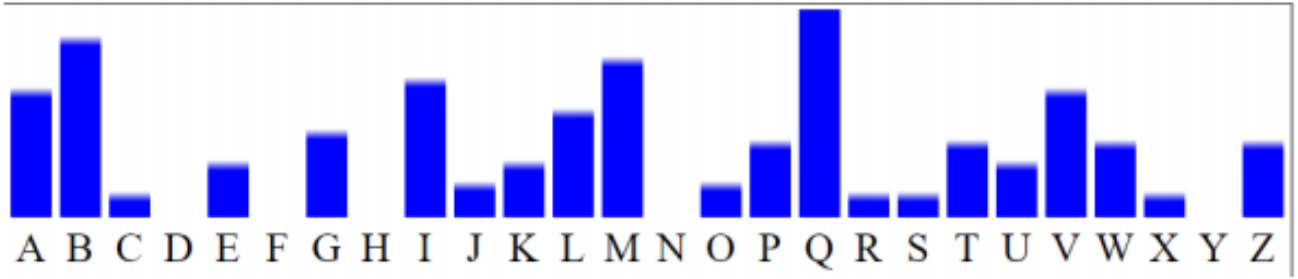
I NEED SAY NOTHING HERE, ON THE FIRST HEAD, BECAUSE NOTHING CAN SHOW BETTER THAN MY HISTORY WHETHER THAT PREDICTION WAS VERIFIED OR FALSIFIED BY THE RESULT. ON THE SECOND BRANCH OF THE QUESTION, I WILL ONLY REMARK, THAT UNLESS I RAN THROUGH THAT PART OF MY INHERITANCE WHILE I WAS STILL A BABY, I HAVE NOT COME INTO IT YET. BUT I DO NOT AT ALL COMPLAIN OF HAVING BEEN KEPT OUT OF THIS PROPERTY; AND IF ANYBODY ELSE SHOULD BE IN THE PRESENT ENJOYMENT OF IT, HE IS HEARTILY WELCOME TO KEEP IT.

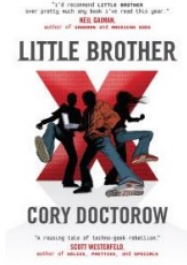
Caesar Cipher-Example 2

UG OIQB EIA ZMKWZLML. BPM KPQX QV UG ABCLMVB QL JZWILKIAB UG QLMVBQBG BW AMVAWZA QV BPM PITTEIG. QB EIA TQSM JMQVO QV RIQT.

Caesar Cipher

- **UG OIQB EIA ZMKWZLML. BPM KPQX QV UG ABCLMVB QL JZWILKIAB UG QLMVBQBG BW AMVAWZA QV BPM PITTEIG. QB EIA TQSM JMQVO QV RIQT.**





- 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
- I J K L **M** N O P Q R S T U V W X Y Z A B C D E F G H
- Encrypt shift right 8
- Decrypt shift left 8
- **MY GAIT WAS RECORDED. THE CHIP IN MY STUDENT ID BROADCAST MY IDENTITY TO SENSORS IN THE HALLWAY. IT WAS LIKE BEING IN JAIL.**

PART II:
Vigenere Cipher

Vigenere Cipher—Example 1

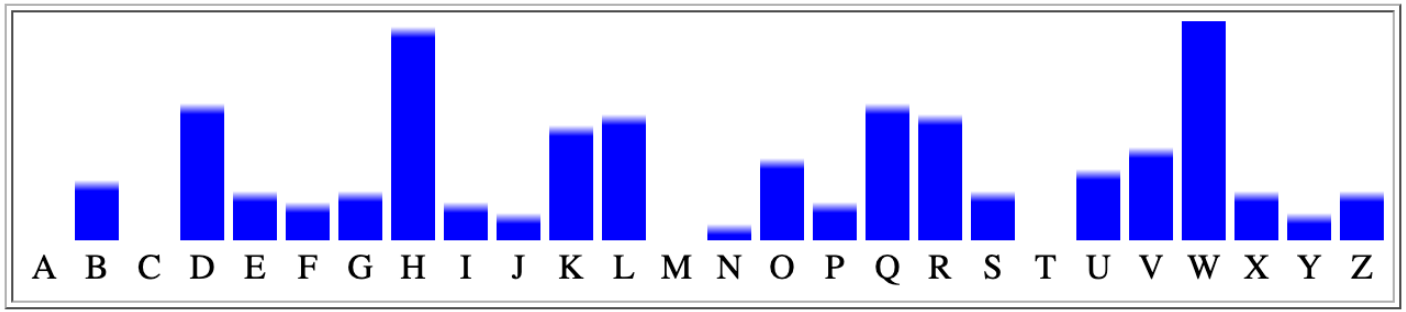
- LUHLGZDFQVWOLUJOHYHVQAKLIPUZWOHHGIHJDBVLQVWOLUJJDUVORDELWAHYWODUPFKPVARYBDKLW
  OHYWODASYHKLJWPRUZHVCHYLMLLGVUMDSVPIPHKEFWOHYHZXSWVQAKLVLFVQKEYDUFORMWOHXXLV
  ALVQPZPOSRUOFULPHURWODAXUOLVZLYDUWOUVXNKAKHWWDYWVITBPQOHYLADUFLZOLSHPZHVZWP
  OSDIDIBPKHYLQVWJRTHPQARPWFHAEBWPGVQVWHWHOSFVPWOHLURMKHYPQNELHUNLSARBWVIAKPV
  WUVSLUABHQKLMDUBIRKBLOZHZKVXSGIHPQAKLSYHZHUWLQQRFPLQARMLAKLLZKLDYWPOFZLOJRTHARR
  HLSPW

- I guess that the key is **two characters** and take every second character to create **two Caesar cipher problems**.
  - **Group 1:**
    LHGDQWLJHHQKIUWHGHDVQWLJDVREWHWDPKVRBKWHWDSHLWRZVHLLGUDVIHEWHHXWQKVFQEDFRWHXVL
    QZOROUPUWDXOVLDWUXKKWDWIBQHLDFZLHZVWODDBKYQWRHQRWHEWGQWWOFPOLRKYQEHNSRWIKVUSUB
    QLDBRBOHKXGHQKSHHWQRPQRLKLKDWOZORHRHSW
  - **Group 2:**
    ULZFVOUOYVALPZOHIJBLVOUJUODLAYOUFPAYDLOYOAYKJPUHCYMLVMSPPKFOYZSVALLVKYUOMOXLAV
    PPSUFLHROAULZYUOVNAHWYVTPOYAULOSPHZPSIIPHLVJTPAPFABPVVHHSVWHUMHPNLULABVAPWVLAH
    KMUIKLZZVSIPALYZULQFLAMALZLYPFLJTARLP

Vigenere 1—Analysis (Group 1)

- LHGDQWLJHHQKIUWHGHDVQWLJDVREWHWDPKVRBKWHWDSHLWRZVHLLGUDVIHE WHHXWQKVFQEDFRWHXVLQZOROUPUWDXOVLDWUXKKWDWIBQHLDFZLHZVWODDB KYQWRHQRWHEWGQWWOFPOLRKYQEHNSRWIKVUSUBQLDBRBOHKXGHQKSHHWQRP QRLKLKDWOZORHRHSW

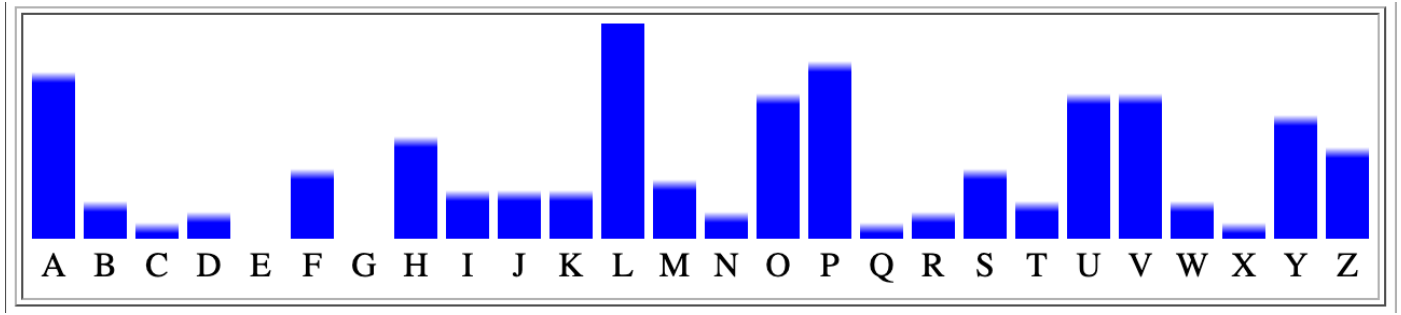
- The **FIRST** letter of the key is "**D**", or a shift to the right **3**
- (i.e. **E->H** for encrypting)
  - A B C D **E** F G H I J K L M N O P Q R S T U V W X Y Z
  - D E F G **H** I J K L M N O P Q R S T U V W X Y Z A B C



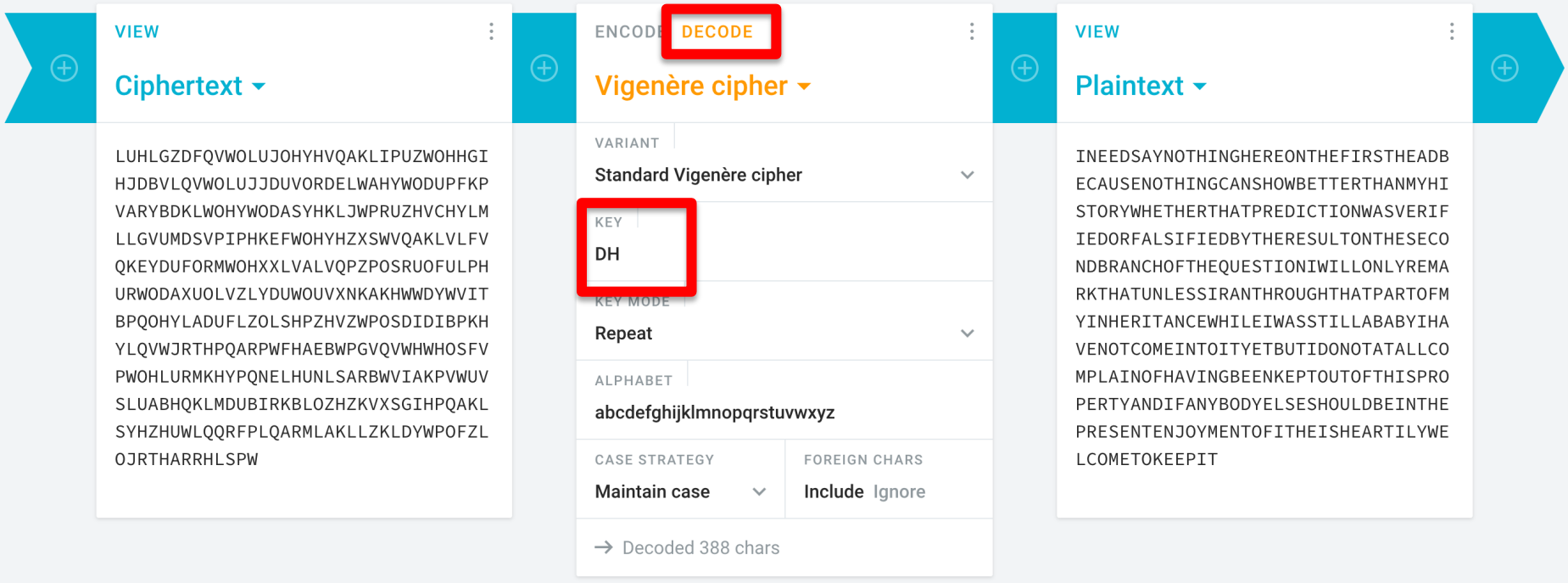
Vigenere 1—Analysis (Group 2)

- ULZFVOUOYVALPZOHIJBLVOUJUODLAYOUFPAYDLOYOAYKJPUHCYMLVMSPPKF
  OYZSVALLVKYUOMOXLAVPPSUFLHROAULZYUOVNAHWYVTPOYAULOSPHZPSIIP
  HLVJTPAPFABPVVHHSVWHUMHPNLULABVAPWVLAHKMUIKLZZVSIPALYZULQFL
  AMALZLYPFLJTARLP

- The **SECOND** letter of the key is "**H**", or a shift to the right **7**
- (i.e. **E->L** for encrypting)
  - 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
  - H I J K **L** M N O P Q R S T U V W X Y Z A B C D E F G



Vigenere 1—Decryption



Vigenere Cipher—Example 2

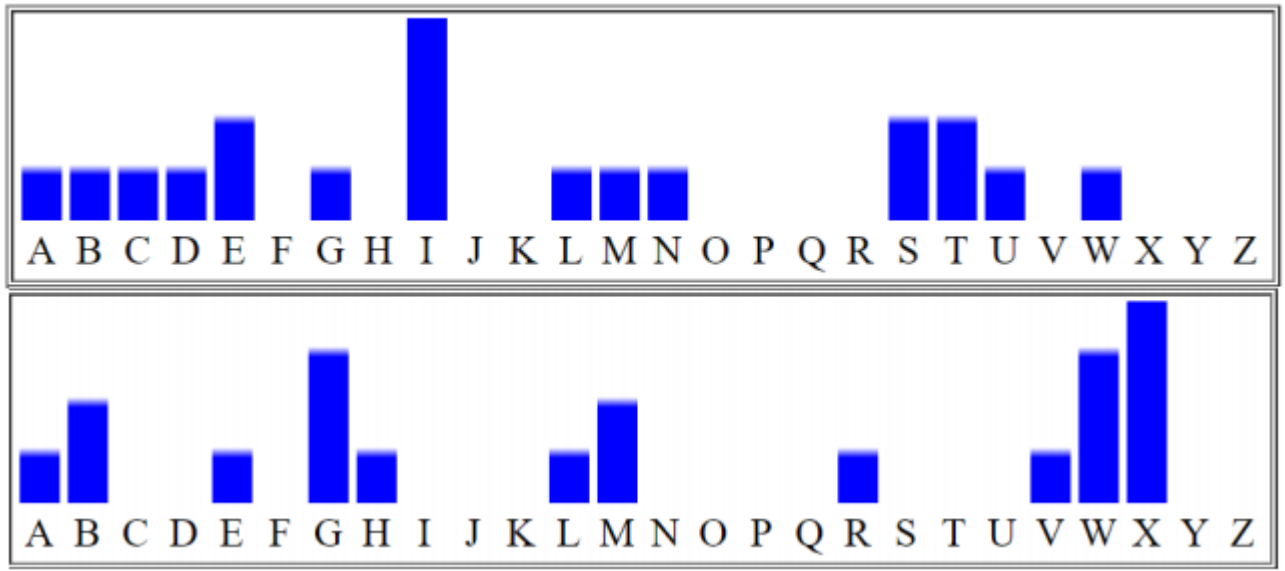
- IM WBLE BX SXEG TAAM I WIW NHT LUVCXEW IG MR DXSBGG.

- I guess that the key is two characters and take every second character to create two Caesar cipher problems.

- **I**M**W**B**L**E**B**X**S**X**E**G**T**A**A**M**I**W**I**W**N**H**T**L**U**V**C**X**E**W**I**G**M**R**D**X**S**B**G**G.
  - Group 1: **IWLBSETAIINTUCEIMDSG**
  - Group 2: MBEXXGAMWWHLVXWGRXBG

Vigenere 2—Analysis

- FREQUENCY ANALYSIS.
- FIRST PROBLEM – **`I`** IS MOST COMMON, FOLLOWED BY E, S, AND T.
- SECOND PROBLEM – **`X`** IS MOST COMMON FOLLOWED BY G AND W.



Vigenere 2—Analysis (cont.)

- IM WBLE BX SXEG TAAM I WIW NHT LUVCXEW IG MR DXSBGG.

- The **FIRST** letter of the key is "**A**" or a shift of **0**:
- (i.e. **E->E** for encrypting,
  - 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
  - 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
- The **SECOND** letter of the key is "**T**", or a shift to the right **19**:
- (i.e. **E->X** for encrypting)
  - ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - TUVWXYZABCDEFGHIJKLMNOPQRS

- IT WILL BE SEEN THAT I DID NOT SUCCEED IN MY DESIGN.
  From "Erewhon" by Samuel Butler (1872).