第一次作业

提交时注明姓名和学号。

一、古典密码部分

1. （5分）利用穷举法破解移位密码。

QGMEMKLTWLZWUZSFYWQGMOAKZLGKWWAFLZWOGJDV

1. （10分）破解代换密码，写出破解过程。

提示：密文A对应的明文为c，每个字母均不会加密为自身。

AZLTBSUZWTCLBCDQFDSKASGDFWOGARTCDZFBSTZSBDABFDAZDBFYDUWOBCSQFWOGFSKLDWZFWUSQOBREZDADOBGDAWGDFRBCWFYDDOBCDFBSZLSKMCWBIRUCBYDAWEEDGAEWFFRAWEAZLTBSUZWTCLBCWBRFSKIDBCSGFSKDOAZLTBRSOBCWBQFDTDOWOGTWTDZSZTDZCWTFFRITEDIDACWORAWEWRGFROBCDDWZELBMDOBRDBCADOBQZLBCDROPDOBRSOSKASITEDJIDACWORAWEWOGDEDABZSIDACWORAWEIWACRODFFQACWFBCDDORUIWZSBSZIWACRODTZSPRGDGISZDFSTCRFBRAWBDGWOGDKKRARDOBIDWOFSKDOAZLTBRSOWOGBCDFQYFDVQDOBROBZSGQABRSOSKDEDABZSORAFWOGASITQBROUCWFWEESMDGDEWYSZWBDFACDIDFSKFBREEUZDWBDZASITEDJRBLISFBSKMCRACWZDDOBRZDELQOFQRBDGBSTDOWOGTWTDZBCDGDPDESTIDOBSKAZLTBSUZWTCLCWFYDDOTWZWEEDEDGYLBCDGDPDESTIDOBSKAZLTBWOWELFRFBCWBRFBCDYZDWNROUSKASGDFWOGARTCDZFBCDGRFASPDZLWOGWTTERAWBRSODWZELSOSKKZDVQDOALWOWELFRFBSBCDZDWGROUSKDOAZLTBDGASIIQORAWBRSOFCWFSOSAAWFRSOWEBDZDGBCDASQZFDSKCRFBSZL

1. （10分）破解 Vigenere 密码。写出Kasiski test 或者重合指数法的破解过程。

DEAXTLICPUVRASMMSTPPJHTCEPNTHTPDTDEHMTHYUDTACJTGDLPCRDKTEGRCLVTGWWRDSSJTPCBWITRCVFXCDVRBPRPOCXQHTDJPMICVCYTXEQAHXHGZSIXKBLPIGUGPCCEPADQPOCDDKAIPALNITPZWWTPLTWTFHRSLYYEIWYAMPZCZAAAROIHEMZSXQJLOETPHTTHROEHTALNITPZDGPUHLBDQAUCXKHGXCYILTPKVUCIQVFEDULRIWCWOLTPKEBPLKIHCRNOXCEAOHAMDACNRPMTHMVNIWCHDKTLAOURPFPIDABRGTLJYPCBNECTPHTXKCHIXHAYEPIGUGPCCEPDCCUTXPJYIHTGUDTBYUDUDPTOGTBHTPRCUTTGQHNSBMYETACJTGXAPTNLCYELXRUEHHGUGPGCCOAJRPOCXLLLTRRYIRRYYSIGSJKHPLKAEEJPACRCZEATAARXRAVMEPLPEHLGSLWPTLTDBCLTIWCKEBPLKWWXJLMDKGUGJHRVWPGBHCPGZVNCTSARPAUVRAS

1. （50分）三个转子的 Enigma 密码机：

要求：提交报告和代码，报告内容包括：算法原理、实际样例的攻击过程和结果、代码文档

必做(1)，其中(2)、(3)两问中选一问作答即可。

初始设置：转子顺序：II- III-I，Ring Setting：D-E-S，Initial Position: A-A-A，接线板：B/X, G/K, W/Y, E/F, P/Q, S/N.

转子内部的接线为：

Rotor I: A-E, B-K, C-M, D-F, E-L, F-G, G-D, H-Q, I-V, J-Z, K-N, L-T, M-O, N-W, O-Y, P-H, Q-X, R-U, S-S, T-P, U-A, V-I, W-B, X-R, Y-C, Z-J.

Rotor II: A-A, B-J, C-D, D-K, E-S, F-I, G-R, H-U, I-X, J-B, K-L, L-H, M-W, N-T, O-M, P-C, Q-Q, R-G, S-Z, T-N, U-P, V-Y, W-F, X-V, Y-O, Z-E.

Rotor III: A-B, B-D, C-F, D-H, E-J, F-L, G-C, H-P, I-R, J-T, K-X, L-V, M-Z, N-N, O-Y, P-E, Q-I, R-W, S-G, T-A, U-K, V-M, W-U, X-S, Y-Q, Z-O.

反射器内部的接线为：A-Y, B-R, C-U, D-H, E-Q, F-S, G-L, H-D, I-P, J-X, K-N, L-G, M-O, N-K, O-M, P-I, Q-E, R-B, S-F, T-Z, U-C, V-W, W-V, X-J, Y-A, Z-T.

1. 编写代码正确模拟Enigma密码机（参考 https://www.101computing.net/enigma-machine-emulator/）。要求密码机可以配置转子顺序（只需要实现I、II、III三个转子）、Ring Setting、Initial Position和接线板。注意理解Ring Setting和Initial Position的含义，每个转子的“进位”位置（Turnover Notch Position）分别为I-Q、II-E、III-V。

测试实现正确性样例：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 转子顺序 | Ring Setting | Initial Position | 接线板 | 明文 | 密文 |
| I-II-III | A-A-A | A-A-A | － | ABCDEF | BJELRQ |
| I-II-III | A-A-A | A-B-T | － | ABCDEF | NYEWVO |
| I-II-III | A-A-A | A-D-U | － | ABCDEF | EEUNGT |
| I-II-III | A-E-S | A-D-U | － | ABCDEF | BCMJMR |
| II-III-I | D-E-S | A-A-A | B/X, G/K, W/Y, E/F, P/Q, S/N | ABCDEF | SDKZQX |

1. 使用波兰人雷臼斯基(Rejewski)的方法，对 Enigma 密码进行破解。需写出原理，并编程实现。可以参考下面的密文的第一个字母和第四个字母，第二个字母和第五个字母，第三个字母和第六个字母的对应表格，找到循环圈。固定RingSetting，恢复转子顺序和 Initial Position (或固定 Initial Position，恢复转子顺序和Ring Setting)。(本题中接线板未知，但不用恢复接线板)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 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 |
| 4 | E | L | C | O | N | W | D | I | A | P | K | S | Z | H | F | B | Q | T | J | Y | R | G | V | X | M | U |
| 2 | 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 |
| 5 | M | R | W | J | F | D | V | S | Q | E | X | U | C | O | N | H | B | I | P | L | T | G | A | Y | Z | K |
| 3 | 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 |
| 6 | W | A | D | F | R | P | O | L | N | T | V | C | H | M | Y | B | J | Q | I | G | E | U | S | K | Z | X |

1. 已知明文：ENIGM ADAIL YSETT INGS...，对应的密文：LVQUK OJOWP NTGHH NGLZ...，找到其中所有的圈，并使用图灵的已知明文攻击的方法，固定Ring Setting，恢复转子顺序和 Initial Position (或固定 Initial Position，恢复转子顺序和RingSetting)。(本题中接线板未知，但不用恢复接线板)

二、完善保密加密

1. （10分）密钥空间的密钥数量严格小于消息空间的消息数量时，可能实现完善保密加密吗？证明你的结论。

2.（15分） One time pad 在多次使用下是不安全的。给定十串明文m1, …, m10，均为英文，用 ASCII编码。随机生成一个pad（密钥），用这个pad加密所有的明文得到密文c1,…,c10。加密方式为pad和明文逐字节异或得到密文。现在你知道所有的密文，恢复密钥，并利用密钥解密目标密文，最终恢复目标明文。

提示：可以把所有的密文取异或，考虑空格的ASCII码是32，和a-zA-Z有区别，利用这个区别恢复明文。

参考：https://crypto.stanford.edu/~dabo/cs255/hw\_and\_proj/hw1.html