# MAS433 Cryptography

# Tutorial 1 Classical Ciphers

08.09.2010

**Problem 1.** Use exhaustive key search to decrypt the following ciphertext, which is encrypted using a shift cipher (hint: the value of the encyption key is less than 7):

FEHJPEWLHVMZIGEYWIHASVWXYWQMPMXEVCFVIEGL

**Problem 2.** Suppose that $\pi$ is the following permutation of $\{1, 2, ..., 8\}$ :

| $x$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $\pi(x)$ | 2 | 4 | 6 | 1 | 8 | 3 | 5 | 7 |

2.1) Compute the permutation table $\pi^{-1}$ (the inverse of $\pi$).

2.2) Decrypt the following ciphertext, which is encrypted using a transposition (permutation) cipher with $m = 8$, and with the key $\pi$ given above.

ETEGENLMDNTNEOORDAHATECOESAHLRMI

**Problem 3.** The ciphertext given in Appendix A is encrypted using a substitution cipher. The statistical data of the ciphertext is given in Appendix B. Try to break the cipher and decrypt the first line of the ciphertext. (In this exercise, the size of the ciphertext is a bit large so that the attack can be relatively easy.)

**Problem 4.** Cipher Composition
4.1) Two substitution ciphers, $S_1$ and $S_2$, are applied to encrypt a message as follows: $c_i = S_2(S_1(p_i))$. Discuss how to attack it.

4.2) Denote the encryption of a Vigenere cipher as $C = V_K(P)$. Two Vigenere ciphers are applied to encrypt a message as follows: $C = V_{K_2}(V_{K_1}(P))$. Discuss how to attack it. Comparing to the attack on $V_{K_1}$ or $V_{K_2}$, does the attack complexity increase? (Hint: consider the Least Common Multiple of the lengths of $K_1$ and $K_2$) Discuss the security of using more than two Vigenere ciphers.

**Problem 5.** If an attacker knows the ciphertext and part of the plaintext, how to attack the shift cipher, substitution cipher and Vigenere cipher, and how to break the composition of Vigenere ciphers in Problem 4.2 efficiently?

# A The ciphertext of Problem 3

JOZYMAZJAJKAWZOYSMZQYWJZAVKMCXYTNYAAEKOBKWCKWYWYEUWAZMDAXZJT

YYBAXKAAXYVOKMUQYWOURYKISMCKRYMAKNFKWWZYWAUAXYOUMAZMSYCWKEZC

RZMZKASWZLKAZUMUIOURESAYWRYRUWVAXKAXKJFYYMAXYFKJZJIUWAXYOUMJ

SRYWYNYOAWUMZOJWYQUNSAZUMZMWYOYMAVYKWJAXYNZRZAJUIEXVJZOJKMCI

ZMKMOYIKOYCFVOXZERKBYWJXKCNUURYCJUNKWDYAXKAYGEYWAJIYKWYCKJNU

TCUTMZMAXYEKOYUIRZMZKASWZLKAZUMAXKATUSNCKOANZBYKFWKBYUMAXYKF

ZNZAVAUEKOBYQYWRUWYEUTYWZMAUYQYWJRKNNYWCYQZOYJNZBYNKEAUEJJRK

WAEXUMYJKMCCZDZAKNOKRYWKJFSAAXYMYTKMMUSMOYRYMAJKNUMDTZAXOURE

YAZMDAYOXMUNUDZYJFYZMDESWJSYCFVOUREKMZYJNZBYZFRKMCZMAYNUIIYW

XUEYAXKAAXYFWKBYTZNNMUAFYKEENZYCKMVAZRYJUUMZMUMYUIAXYATUMYTC

YQYNUERYMAJWZOYWYJYKWOXYWJKWYWYEUWAZMDZMMKMUNYAAYWJKPUSWMKNU

IAXYKRYWZOKMOXYRZOKNJUOZYAVAXKAAXYVXKQYJSOOYYCYCZMFSZNCZMDWY

NZKFNYJRKNNCZDZAKNJTZAOXYJKMYJJYMAZKNEKWAUIOURESAYWRYRUWVAXK

AOUSNCJXWZMBAUKJZDMZIZOKMANVJRKNNYWJOKNYAXKMZJEUJJZFNYSJZMDO

UMQYMAZUMKNRYAXUCJRUWYZREUWAKMAAXYKCQKMOYZJFKJYCUMJZNZOUMUGZ

CYUMYUIAXYFKJZOFSZNCZMDFNUOBJUIAUCKVJOXZEZMCSJAWVAXSJYKJZMDK

RUQYAUTKWCOURRYWOZKNZLKAZUMAXYJOZYMAZJAJJKZCAXKAEWZQKAWKMKAY

GKJJAKWASEOUREKMVXKJRKCYYGEYWZRYMAKNOXZEJSJZMDAXYAYOXMZHSYAX

KAOKMJAUWYKMCWYAWZYQYZMIUWRKAZUMAXZJZJJURYAXZMDAXKAZFRJASCZY

CFYIUWYKMCTXZOXZJJAZNNZMAXYWYJYKWOXJAKDYJKZCOXKWNYJNKRKMZFRJ

EYOZKNZJAZMJYRZOUMCSOAUWRYRUWZYJXEXKJIUWJYQYWKNVYKWJFYYMRKBZ

MDONKZRJAXKAZAJRYRWZJAUWAYOXMUNUDVOKMOUREYAYTZAXAWKCZAZUMKNA

WKMJZJAUWJFSAAXYOUREKMVTZNNWYEUWAAXZJTYYBAXKAZAZJMUTRUWYOUMI

ZCYMAAXKAZAJAYOXMUNUDVOKMOUREYAYOURRYWOZKNNVZMAXYISASWYZMOUM

```
AWKJAAXYWZOYKCQKMOYRSJAJAZNNFYEWUQYCKOBMUTNYCDZMDAXKAWYJYKWO

XYWJRSJAUQYWOURYJBYEAZOZJRFYOKSJYJZNZOUMUGZCYXKJFYYMBMUTMKJK

MZMJSNKAUWFVAXYZMCSJAWVSMAZNMUTPZRAUSWKMKMURKAYWZKNJJEYOZKNZ

JAKAWZOYJKZCXYFYNZYQYCAXYZMCSJAWVTUSNCXKQYAUNUUBJYWZUSJNVKAA

XYWYJYKWOXAYKRJMYTKEEWUKOXZAJKXKWCJYNNFYOKSJYKAIZWJAZAJUFQZU

SJZATUMATUWBXYJKZCFSARVXUEYZJAXKAAXZJZJJUJZRENYAXYVTZNNXKQYA

UESAZAZMAXYZWEUWAIUNZUAUYGENUWY
```

## B The statistical data of the ciphertext of Problem 3

The probabilities of the letters:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| A | 0.0983 | B | 0.0098 | C | 0.0289 | D | 0.0120 | E | 0.0257 |
| F | 0.0175 | G | 0.0033 | H | 0.0005 | I | 0.0126 | J | 0.0705 |
| K | 0.0847 | L | 0.0016 | M | 0.0672 | N | 0.0431 | O | 0.0442 |
| P | 0.0011 | Q | 0.0115 | R | 0.0350 | S | 0.0240 | T | 0.0142 |
| U | 0.0699 | V | 0.0147 | W | 0.0584 | X | 0.0464 | Y | 0.1158 |
| Z | 0.0890 | | | | | | | | |

The frequency of the occurrence of the most frequent digrams:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| AX | 51 | ZM | 34 | XY | 32 | YW | 32 | KM | 30 |
| KA | 29 | AZ | 28 | MA | 27 | XK | 26 | UM | 25 |
| JA | 23 | UW | 22 | WY | 22 | OU | 21 | YJ | 21 |
| KN | 20 | RY | 19 | YA | 19 | YK | 19 | ZJ | 19 |
| AU | 18 | KW | 18 | WZ | 17 | JZ | 16 | MU | 16 |
| OX | 16 | ZA | 16 | ZO | 16 | NZ | 15 | QY | 15 |
| UR | 15 | YO | 15 | AY | 14 | KJ | 14 | YM | 14 |
| AA | 13 | JK | 13 | JY | 13 | MD | 13 | MZ | 13 |
| OY | 13 | WJ | 13 | YC | 13 | AW | 12 | NU | 12 |
| SJ | 12 | WA | 12 | AJ | 11 | MC | 11 | NY | 11 |
| OK | 11 | RK | 11 | XZ | 11 | ZN | 11 | ZY | 11 |
| FY | 10 | NN | 10 | RE | 10 | WK | 10 | YZ | 10 |
| ZU | 10 | EY | 9 | JJ | 9 | JR | 9 | UI | 9 |
| ZK | 9 | AK | 8 | BY | 8 | CZ | 8 | JU | 8 |
| MK | 8 | MO | 8 | OZ | 8 | SA | 8 | UN | 8 |
| US | 8 | UT | 8 | WO | 8 | YN | 8 | YQ | 8 |
| YR | 8 | ZC | 8 | | | | | | |

The frequency of the occurrence of the most frequent trigrams:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| AXY | 25 | AXK | 17 | XKA | 15 | OUR | 12 | ZMD | 12 |
| AAX | 11 | YMA | 11 | MAX | 9 | KAZ | 8 | OUM | 8 |
| URE | 8 | AZU | 7 | UMA | 7 | UWA | 7 | XAX | 7 |
| YKW | 7 | YWJ | 7 | ZJA | 7 | ZUM | 7 | | |