

Computer Tutorial 3

Start MAGMA, type `SetLogFile("ctut3.txt");` and type `load "tut3data.txt";`.

A *translation cipher* is a substitution cipher in which each letter is replaced by the letter that occurs k steps later in the alphabet. More precisely, the i th letter of the alphabet is replaced everywhere by the j th letter, where $j \equiv i + k \pmod{26}$. (The case $k = 3$ is *Caesar's Cipher*. The case $k = 1$ occurred in Question 3 of Computer Tutorial 2.) A translation cipher is completely determined by the letter that replaces A, and so it is traditional to call this single letter the key.

A *Vigenère cipher* is constructed from n translation ciphers. To encipher the first letter of a message the first cipher is used, for the second letter the second cipher is used, and so on; for the $(n + 1)$ st letter you return to the first cipher. To be precise, the i th letter of the message is enciphered with the j th translation cipher, where $j \equiv i \pmod{n}$. For a Vigenère cipher the key is the n -letter word made up of the keys of the n translation ciphers.

1. Type `V:=VigenereCryptosystem(7);` and `k:=V!"CARSLAW";`, and then encipher a message. (For example: `M:="Computer Tutorial Three";`, then `P:=Encoding(V,M);` and `C:=Enciphering(k,P);` would do.) Get MAGMA to print your enciphered message and check that it is right. (If you need them, commands like `alphabet[15];` and `Index(alphabet,"S");` can be used to find out where various letters occur in the alphabet.) Type `m:=InverseKey(k);`, then print `m` and check that it is right. Check that `Enciphering(m,C);` recovers `P`. (Incidentally, why is there a 7 in the definition of `V`?)

The probability that two randomly chosen letters from a piece of text are the same is called the *coincidence index* for the text. Suppose there are N letters in the text, of which N_1 are A's, N_2 are B's, and so on. So $N = \sum_{i=1}^{26} N_i$. Let $p_i = N_i/N$. If we choose a letter at random then the probability that it is an A is p_1 , the probability that it is a B is p_2 , and so on. If we choose one letter and then independently choose another then the probability that they are both A's is p_1^2 , and the probability that they are both B's is p_2^2 , and so on. The probability that the two randomly chosen letters are the same is the probability that they are both A's plus the probability that they are both B's plus ... plus the probability that they are both Z's. That is, the coincidence index is $\sum_{i=1}^{26} p_i^2$. For a random string of letters from a 26 letter alphabet the expected value of the CI is $1/26 \approx 0.0385$, but for English text it is usually about 0.066. (Why the difference?)

2. The file `tut3data.txt` that you have loaded contains an excerpt from the short story "The Dancing Men" by Sir Arthur Conan-Doyle. Type `dancemen;` to see it. Then type `CoincidenceIndex(dancemen);`, and observe that the answer is close to typical. Now type `S:=SubstitutionCryptosystem();` followed by `dm:=Encoding(S,dancemen);`, `rk:=RandomKey(S);`, `rk;` and `cdm:=Enciphering(rk,dm);`. Get MAGMA to tell you `CoincidenceIndex(cdm)`, and compare the result with the CI of the unenciphered text. Repeat the commands from `rk:=RandomKey(S);` onwards a few times to obtain the CI for a few different encipherings. Can you explain the results?

Now use the Vigenère cipher from Exercise 1: type `dmv:=Encoding(V,dancemen);` and `cdmv:=Enciphering(k,dmv);`, then type `CoincidenceIndex(cdmv);`. Then do `k:=RandomKey(V);`, encipher `dmv` with this new key and find the CI. Can you explain why the CI is still greater than $\frac{1}{26}$? Would choosing a longer Vigenère period reduce the CI? Try it and see! (Start with the commands `VV:=VigenereCryptosystem(20);` and `dmvv:=Encoding(VV,dancemen);`.)

The file `tut3data.txt` contains some Vigenère-enciphered ciphertexts, named `vt1`, `vt2`, `vt3` and `vt4`. In the remaining exercises we shall attempt to decipher them via frequency analysis. Our main tool is a function called `Decimation` that is defined in our MAGMA cryptography package. (Note that decimating a population literally meant killing every tenth person).

3. Try to figure out what the `Decimation` function does: type


```
alph:="ABCDEFGHIJKLMNOPQRSTUVWXYZ";
Decimation(alph,1,3);
Decimation(alph,2,3);
Decimation(alph,2,6);
```

 and examine the output. (There is a bug: it doesn't print as many terms as it should.)
4. All objects that MAGMA works with must have a "type". For example, `dm` and `cdmv` above are, in MAGMA's opinion, objects of type "CryptTxt", while `k` and `rk` are of type "CryptKey". (Type the command `Type(dm);`.) A string of characters, such as `alph` above, is an object of some other type. (Type `Type(alph);`.) The `Decimation` function can only be used on strings, not on cryptographic text. However, in the next exercise we shall want to decimate `cdmv`. So that we can do so, type `scdmv:=String(cdmv);` to create a string `scdmv` consisting of the same letters as `cdmv`. Check that `vt1`, `vt2`, `vt3` and `vt4` are already strings.
5. Before starting work on `vt1` let us examine decimations of the ciphertext `cdmv`; . Recall that the Vigenère period for `V` is 7. Type


```
CoincidenceIndex(Decimation(scdmv,1,7));
CoincidenceIndex(Decimation(scdmv,2,7));
CoincidenceIndex(Decimation(scdmv,3,7));
```

 Do the same again using a decimation period that is not equal to the Vigenère period. (For example, use the same commands with 6 instead of 7.) Repeat for several choices of the decimation period. What do you observe?
6. We now try to find the Vigenère period for `vt1` by checking the CI for decimations of periods from 2 to 20. Type


```
for i:=2 to 20 do
  print "Period:",i,"CI:",CoincidenceIndex(Decimation(vt1,1,i));
end for;
```
7. The output from the above commands should enable you to correctly deduce that the Vigenère period for `vt1` is 13. Use `SortedFreqDist(Decimation(vt1,1,13));` to find which letter occurs most frequently in this decimation. This letter presumably represents E in the first of the 13 translation ciphers that make up the Vigenère cipher. Work out what represents A. Repeat this idea for `Decimation(vt1,i,13)`, for all values of `i` from 1 to 13, and hence determine the key.
8. Type `V1:=VigenereCryptosystem(13);` and `k1:=V1!"BATMANFOREVER";` to define `k1` to be the key you (should have) found in the previous exercise. Then type the command `Enciphering(InverseKey(k1),Encoding(V1,vt1));` and you should get something readable.
9. Do the same for `vt2`, `vt3` and `vt4`. (Be warned that sometimes the most frequent letter in a decimation does not represent E. So you should check the assumption that it does by looking at some other frequencies. For example, in one case the most frequent letter is B, followed by I and M. If B represents E then I represents L and M represents P. This can't be right: maybe L could be the second most frequent letter in some unusual piece, but surely P cannot be the third most frequent letter! If I represents E then B represents X. This can't be right either. In fact M represents E, which means that B represents T and I represents A.)