Information Systems Security
Exercices Series 3 Correction : Historical Ciphers

October 13th, 2021

Exercice 1: Simple Encryptions and Decryptions

1. The "H" is replaced with a "M" (+ 5 letters).
   Similarly, "E" becomes a "J", both "L" become "Q", and so on.
   The complete ciphertext is "MJQQTBTWQI".

2. The key is "ILOVECRYPTGAHBDFJKMNQSUWXZ". That means "A" is replaced with "I", "B" is replaced with "L", ...
   We encrypt the "S" as a "M" ("S" is the 19th letter in the alphabet, and is replaced with the 19th letter of the key, which is "M"),
   The "U" becomes a "Q",
   The "B" becomes a "L",
   And so on. We obtain the ciphertext "MQLMNPNQNPDB".

3. The "E" was originally a "C" (as "E" is the third character of the key, that was originally the third character of the alphabet)..
   Similarly, the "O" was a "I", the "H" was a "P", ...
   We find the original message : "ciphertext".

4. We have Y+C = 24+2 mod 26 = 26 mod 26 = 0 = A,
   then O+E = 14+4 mod 26 = 18 = S,
   U+N = 20+13 mod 26 = 33 mod 26 = 7 = H,
   And so on.
   We find the following cipher : "ASHCCRGSGIZE".

5. We have X-P = 23-15 mod 26 = 8 = I,
   I-I = 8-8 mod 26 = 0 = A,
   W-K = 22-10 mod 26 = 12 = M,
   A-A = 0-0 mod 26 = 0 = A,
   R-C = 17-2 mod 26 = 15 = P,
   V-H = 21-7 mod 26 = 14 = O,
   E-U = 4-20 mod 26 = -16 mod 26 = 10 mod 26 = K,
   And so on.
   The original message was "IAMAPOKEMONMASTER".

Exercice 2 : Breaking Monoalphabetical Ciphers

1. The most simple way is to test all possibilities. We can easily see that for keys 1,2 and 3, that would be a message that can be understood. Foe example, if w suppose the key was 1 (each letter was replaced by the next one), then the first word would have been ”VHFXULWB”. That doesn’t seem like the message. Same ting for keys 2 and 3.
   But for key k=4, we find as first word ”SECURITY”. That seems like our meaningful message. With that key, we obtain the full message ”SECURITY IS GUARANTEED WITH THIS CIPHER” (and it seems Cesar underestimated you).

2. With frequential analysis, for example with the english language, we know that the ”E” has by far the biggest frequency. So we can imagine that the letter that is the most frequent in the cipher was originally a ”E”. We can even compute distancies with every frequency in our ciphertext to find which key is the most probable (the same way as the frequential analysis in vigenere, in exercice 3).

3. By analysing the text and the specific structures (if we still have ponctuation, we can analyse what letters are a word by themselves, or are alone after/before an apostrophe, or which letters are doubled in some words, etc...), and by comparing frequencies with the ones of the expected language, we can easily find the most frequent letters like ”e” or ”a” or ”s” for example. With the help of smaller words, we can easily find a few letters. AS soon as we have a few letters, we can find the rest by completing words that are missing only one or two letters. That allows us to break monoalphabetical encryption by hand in a few minutes (aside from counting frequencies).

4. As these two encryption methods are easily breakable by hand, they’re not secure at all.

Exercice 3 : Breaking Vigenere’s Cipher

The original key was ”DREAD” (Though with the formula, you’re suppose to find the key ”DREADDREAD” of length 10).
The original text was the following :

”themetroidgamesareaseriesofvideogamesproducedbynintendooneofthecompanys mostsuccessfulfranchisestheseriespopularityspansseveralnintendoconsoles withthefirstgamemetroidreleasedinnineteeneightysixforthenintendo entertainmentsystemthemetroidgameschroniclethemissionsofbountyhunter samusaraninasciencefictionsettingwhichcontainsmanysimilaritiestothealien filmfranchisecentralplotelementsarethemetroidorganismsandthespacepirates whichtrytoexploitthemetroidspowersthegameplaycombinesadventurebasedon explorationanditemgatheringwithplatformerandshooterdynamicsthemetroid gamesarefamousfortheirnonlineargameplaywhereonecancompleteagamewitha fractionoftheitemsavailableinthegametherearеoveradozengamesintheseries thisincludesfivemaingamesmetroidmetroidtworeturnofsamussupermetroid metroidfusionandmetroiddreadtwospinoffgamesforthenintendodsfamily metroidprimepinballandmetroidprimefederationforceafirstpersonadventure gamewithwirelessandonlinemultiplayermetroidprimehuntersthemetroidprime trilogymetroidprimemetroidprimetwoechoesandmetroidprimethreecorruption andmetroidothermaswellasvariousotherportsandremakes ”

Conclusion : Vigenere’s cipher is not really secure either (unless you use it as a one-time pad method with keys of the same length as the text used only once).