Spring 2023

MATH 1025: Introduction to Cryptography

Homework 3

RSA

Problem 1. Let us practice with the RSA cryptosystem (use the programs http://tsvboris.pythonanywhere.com/IntrotoCryptography).

(a) [10 **pts**] My number n is 171352770689 and encryption key $e = 58787$. Using the encoding given by the correspondence $A \leftrightarrow 11, B \leftrightarrow 12, \ldots, Z \leftrightarrow 36$, send me a short message (the plaintext must be meaningful and contain at least six letters, each five letter block should be converted to the corresponding 10-digit number, the last block can contain any $0 < k \leq 5$ number of letters and is converted to an at most 10-digit number).

(b) [10 **pts**] Find the factorization of n and my decryption exponent d. A grateful student sent me a message

$$'52284131866|29526308836'.$$

Hope it is something good. Let me know (decrypt the message).

Problem 2 [10 **pts**] Bob and Alice use a cryptosystem in which their shared key is a (large) prime k and their plaintexts and ciphertexts are integers. Bob encrypts a message m by computing the product $c = km$. Eve intercepts the following two ciphertexts: $c_1 = 12849217045006222, c_2 = 6485880443666222$. Find the shared key k.[1]

Frequency analysis

Problem 3**.**

(a) [10 **pts**] How many strings of length $\ell > 1$ have index of coincidence equal to 1?

(b) [10 **pts**] How many strings of length ℓ have index of coincidence equal to 0?

(1) $1 \leq \ell \leq 26$

(2) $\ell \geq 27$

[1] **Hint:** use a program (http://tsvboris.pythonanywhere.com/IntrotoCryptography) to find $\gcd(c_1, c_2)$. Notice that $\gcd(c_1, c_2) = \gcd(km_1, km_2) = k \cdot \gcd(m_1, m_2)$ is divisible by k. Then use another program to factor $\gcd(c_1, c_2)$ and find k.

(c) [10 **pts**] Let $s_\ell = \underbrace{aa\ldots a}_{\ell}\underbrace{bb\ldots b}_{\ell}$ and find the limit $\lim_{\ell\to\infty} \mathrm{IndCo}(s_\ell)$.

(d)* [5 **pts**] For a given $1 \le n \le 26$, find a family of strings s_ℓ, s.t. $\lim_{\ell\to\infty} \mathrm{IndCo}(s_\ell) = \frac{1}{n}$.

Problem 4**.**

(a) [10 **pts**] How many pairs of strings of lengths n and m have mutual index of coincidence equal to 1?

(b) [10 **pts**] Give an example of a pair of strings (s,t) with $\mathrm{MutIndCo}(s,t) = 0$

(c) [15 **pts**] Let s and t be two strings of lengths $m = \ell en(s) \ge 1$ and $n = \ell en(t) \ge 1$, s.t. $\mathrm{IndCo}(s) = \mathrm{IndCo}(t) = \mathrm{MutIndCo}(s,t) = 0$. What is the maximal value of $m+n$? (explain your answer)

Vigenère cipher

Problem 5. A very important encryption was intercepted. It was encrypted using a Vigenère cipher. The message reads:

'Aa mj l qczaaec xwudsri kz hjogymqp pgpgyi fys jkk kekl. Wpcwuwzmza yfl fvrwpc lv xntgv psjxj ec ueaa xypctswz, medhgkv vj kssqbalw kz gwsl meteg Yrwu cff vcfw lpzxwpkllh kss kwhvwjtpno, ooekpjgb jlqrtbu, rgdimpf kwhysslpno, ebwk ms vrw avlev'

(a) [20 **pts**] Let ℓ be the length of the keyword. Using the procedure outlined in Step 1, page 3 of 'Lectures14 – 16' file, a program for computing the index of coincidence for a given string (http://tsvboris.pythonanywhere.com/IntrotoCryptography) and given that $4 \leq \ell \leq 10$, find ℓ. Enter your answer at http://tsvboris.pythonanywhere.com/IntrotoCryptography to get the keyword. **You must provide the indices of coincidence for each possible value of $4 \leq \ell \leq 9$ and motivate your choice, in order to receive credit.**

(b) [10 **pts**] Use the keyword to decrypt the ciphertext (in order to get the original text back, you need to **add** the numbers corresponding to the letters of the keyword to those of the ciphertext letters, the correspondence is $A \leftrightarrow 0, B \leftrightarrow 1, \ldots, Z \leftrightarrow 25$).