National Technical University of Athens
School of Electrical and Computer Engineering

Computational Cryptography
1st Set of Exercises

Submission Deadline: November 15, 2024

Exercise 1. Consider the affine cipher: $c = \mathsf{Enc}((a, b), m) = (ax + b) \mod 26$.
We assume that the adversary (not knowing a, b) can choose two messages m_1, m_2 and obtain their encryptions c_1, c_2 (CPA–Chosen Plaintext Attack).

1. How can the adversary use this capability to break the cryptosystem? How will they choose m_1, m_2;
2. Let's assume that, for increased security, we decide to use double encryption with different keys, namely:
$$\mathsf{Enc}(((a_1, b_1), (a_2, b_2), m) = \mathsf{Enc}((a_2, b_2), \mathsf{Enc}((a_1, b_1), m))$$
   - How does the key space change (if it does) in an exhaustive search?
   - Is the new cryptosystem more secure?

   Justify your answers.

Exercise 2.
Write a program in Python, C/C++, or another language of your choice, using the standard libraries, which takes encrypted text encrypted with Vigenère as input and outputs at most 5 possible plaintexts and their corresponding keys. One of these should be identical to the correct one, with all letters in the right positions. Your program should also calculate the index of coincidence for each plaintext.
Explain the basic ideas used in your code.
Input ciphertext:

jpig ysthxucwmqs yhw gpmksq aleea sec, zg sisb lbr zqti nvh mgw nhor wj ahk jvqr, irw vwpa mabs mgw ovyabebmk. voiem lx dflvcrl lbr krpvvb egc kqsmgchx, zff mse big xwcyw qqh gnl yleeg sy hl. dbx nb ptrl jpw umeks ujhrtmh,-tmv tpwvvk hmw ovvaqrz vavo xum vhrq fhaa, pi pdfv iiswvx szg zya, irw rhcri gpyl tfvv mg: blht ytleg axtq! ojhx jwyec tg all peioaplwf qj mggw oeqax gnl vosfm jhq ojvq gpsn rzkuifb! jhq lgu crivl gsua xuwy vkaoiiq pmmgwt brgw qr bsxl: xuwy pnmnkwg peod oghvvmh he ljf pvolm zff vj gpi cnmtuil, pew hl pvx omig egt ti, zqrx dsisi, nvh fx kgytrvx. utl yl ejimmdv voir mzxqq ovvaqrz, sgqr jewq mgwg alvvi huwtmpbe egc tnlwfmh mgwg mse qx. en! a ct arivr nx of avahhl, dkri gpi udw voeg pemg ycalrziw sgq typp lhmwa; p rrmh azffz shbwmqwvjlrl xh ssml mg. q ahtdf mevv fxrlqd eal hbrltpfhbi, nmlks xum abrw jhzr wrvd eqyi omghlw lvcbcw bm ljlme nsekq, cuh gpi ingt oecxc bm ljlme zmvgwu. alrziynjg tyfb m wdkelrq qrmn ljl hrmt: tr ljvy qwils ap alr mzxmapn, aumr mggw nsrax udzkuh gpi lds, cuh tqzxrl npkub eerg vv xum rxszgy-abzpw, szqb ikcfxqspa wgiv! ehcg alrm qnrl k ns qwag, zk olr fic, mn ojvq v altkd flwpmrw. adgzw zm, xadf, vosh bvtmiwpp rgi, mgsv jeaax udzqsh rdig szg nvrixxrl jhtcqrxrk ypxuwym dfxf! fymwl szg jyc blts au hfbcx mn gxlvstsp, szca xum atswt tel nphv yqshrv sns gh px, nvh vzjtf iimvrvzgyi gpi kdxnlggqsg nx voc otmlr! dq! alva gno au hknqr znapn xb mqisq kawrtj, tmv bhvnblnrlth mf ikthf ivmao xh aw c tea. blnr tgnea hekzljbwgze'l cgyu-kbqrz.

The format of the program's output should be as follows:

KEY1 PLAINTEXT1 IC1
KEY2 PLAINTEXT2 IC2
KEY3 PLAINTEXT3 IC3

... (etc., a total of up to 5 lines of this format)

Note: Alternative approaches are acceptable, possibly with reduced scoring, as long as you explicitly mention them. For example, using the online coincidence index calculator that you can find here: `https://www.dcode.fr/index-coincidence`. The use of a Vigenère solver is not allowed.

Exercise 3.

1. In a cryptosystem that possesses perfect secrecy, is it necessary for every key to be chosen with the same probability? Is it necessary that the key spaces be equiprobable? Provide proof for your claims.
2. Prove that the following statements are equivalent to Shannon's perfect secrecy condition:
   i. $\forall x \in \mathcal{M}, y \in \mathcal{C} : \Pr[C = y] = \Pr[C = y | M = x]$
   ii. $\forall x_1, x_2 \in \mathcal{M}, y \in \mathcal{C} : \Pr[C = y | M = x_1] = \Pr[C = y | M = x_2]$

Exercise 4.

Alice uses the one-time pad and realizes that when her key is $k = 0^\lambda$ (all zeros), then $\mathsf{Enc}(k, m) = m$. In other words, the message is sent without any encryption!

To address the above problem, she modifies the key generation algorithm of the one-time pad so that the key is uniformly chosen from $\{0,1\}^\lambda \setminus 0^\lambda$. In other words, the key can be any binary string of length λ without considering the string consisting of λ zeros.

Is this modified one-time pad still perfectly secure? Justify your answer.

Exercise 5. Let us define the multiplicative version of the one-time pad. Specifically, if p is prime, the encryption of plaintext m with key k ($m, k \in \mathbb{Z}_p^*$) is defined as $\mathsf{Enc}(k, m) = (k \cdot m) \bmod p$.

1. Define the decryption function.
2. Prove the correctness of the system (i.e., that every decryption yields the correct original message).
3. Does this modified one-time pad remain perfectly secure? Justify your answer.

Exercise 6.

1. Suppose that $2^n - 1$ is prime. Prove that n is prime.
2. Let $p \in \mathbb{N}^+$ be an odd prime, and $M_p = 2^p - 1$.
   i. Show that $M_p \equiv 1 \pmod{p}$.
   ii. Show that $p \mid \varphi(M_p)$.
3. Prove that if p and q are distinct primes, then $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.
4. Let $p > 2$ be a prime number. Prove that:
$$\sum_{\beta \in \mathbb{Z}_p^*} \beta = \sum_{\beta \in \mathbb{Z}_p^*} \beta^{-1} \equiv 0 \pmod{p}.$$
5. Consider an integer $n > 2$. Prove that n is a prime iff:
$$(n-1)! \equiv -1 \pmod{n}.$$

Exercise 7. Let $(\mathbb{G}_1, +_1)$ and $(\mathbb{G}_2, +_2)$ be abelian groups, and $\mathbb{B}$ a subgroup of $(\mathbb{G}_1 \times \mathbb{G}_2, +)$, where the operation $+$ is defined as:
$$(a_1, b_1) + (a_2, b_2) = (a_1 +_1 a_2, b_1 +_2 b_2)$$
Furthermore, let
$$\mathbb{B}_1 = \{a_1 \in \mathbb{G}_1 : (a_1, b_1) \in \mathbb{B} \text{ for some } b_1 \in \mathbb{G}_2\}.$$
Show that $(\mathbb{B}_1, +_1$ is a subgroup of $\mathbb{G}_1$.

Exercise 8. Let $\mathbb{Z}_p^*$ be a group with p prime and g a generator, where p and g are known.

1. If d is an integer that divides $p-1$, efficiently find an element b in $\mathbb{Z}_p^*$ of order d (i.e., the smallest integer d for which $b^d \equiv 1 \pmod{p}$).
2. How many elements of order d exist in $\mathbb{Z}_p^*$?
3. How many generators does the cyclic subgroup generated by an element b of order d have?
4. How many cyclic subgroups of order d exist in $\mathbb{Z}_p^*$?
5. Given an element h, the order of d, and a random element a, how can we determine in polynomial time whether a belongs to the subgroup generated by h?

Exercise 9. Write a program to implement the Miller-Rabin primality test (your program should support operations with large numbers, possibly with thousands of digits). Apply it to check the primality of the following numbers:
$67280421310721, 170141183460469231731687303715884105 7, 2^{1001}-1, 2^{2281}-1, 2^{9941}-1.$

Bonus Exercise (no strict deadline)

The Game of the Iron Throne

Many years ago, in the distant town of King's Landing, there lived Geoffrey the Unlikable with his subjects. In total, there were $2^{19}-1$ people, and each of them had one mortal enemy, except for Kallikatzaros, who was liked by everyone.

Each of them had a personal knife (all knives were different from each other), and each one had wounded every other with some knife. Eventually, they all got wounded by all the knives (specifically, each person's knife was used by someone else to wound that person).

Kallikatzaros, whom each person wounded with some knife, had a knife that everyone used to wound themselves. Also, Kallikatzaros wounded every person with the knife of that person's mortal enemy, and since Kallikatzaros didn't have a mortal enemy, he wounded himself with his own knife.

Moreover, for every three people, the person who wounded the third using the knife of the one who wounded the second with the knife of the first, is the same person who used the knife of the first to wound the one who wounded the third with the knife of the second.

1. If Dragonmother was the one who wounded John Snow with the knife of Geoffrey the Unlikable, who wounded Geoffrey the Unlikable with the knife of John Snow?
2. If we know that Dragonmother and Geoffrey the Unlikable are mortal enemies, who wounded Dragonmother with her knife?
3. Who used the knife of the person who wounded John Snow with John Snow's knife to wound the one who wounded Geoffrey the Unlikable with Geoffrey's knife?

Hint: As strange as this exercise may seem, yet it has a strictly mathematical solution. Try to find it without looking at the footnote. [1]

Short instructions: (a) try on your own, (b) discuss with your fellow students, (c) search for ideas on the internet—in this order and after dedicating enough time to each stage! In any case, the answers must be *strictly individual*. You may be asked to present some of your solutions soon.

Good luck!

[1] Try to define a suitable group operation that expresses that x wounded y with the knife of z.