Homework 1

- Questions from Lecture unit 1
- Please refer to the lecture slides for more information about the context in which the questions arise.
- Due date: September 4, 2019

Questions

1. Why do you think keyed cryptography is more practical nowadays?

2. Shift cipher can be generalized where the encryption function is of the form
$$E(x) = ax + b \mod 26$$
for $x \in \{0, ...25\}$, where $a, b \in \mathbb{Z}$. The encryption function needs to be injective (one-to-one) so that every ciphertext can be uniquely decrypted. What conditions should be posed on a and b in order for E to be injective?

3. Is $\Gamma = \begin{pmatrix} 7 & 14 \\ 3 & 23 \end{pmatrix}$ invertible? If so, what is Γ^{-1} (so that $\Gamma^{-1}\Gamma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$?

4. Let's say it takes a second to try a key, that is an m by m matrix Γ, where we will need to construct its "inverse" Γ^{-1} and use it to try to decrypt a ciphertext. Supposedly we may need to try all possible m by m matrices. How small can m be so that it will take us at least 1000 years to try all keys in order to break the cipher?

5. Which do you think is a stronger evidence for security?
   (a) Matrix-cipher: exhaustively trying all possible keys takes too much time (26^{m^2}).
   (b) RSA: Breaking the system may require factoring integers, a problem believed to be computationally hard.

6. Suppose

(a) $Pr[b = 1] = 2/3$ and $Pr[b = 0] = 1/3$.

(b) r is generated with the following probability, independently of what b is: $Pr[r = 1] = Pr[r = 0] = 1/2$.

Questions:

(a) What is the probability that $c = b \wedge r$ is 1?

(b) What is the probability that $c = b \wedge r$ is 0?

(c) Is it a good idea to hide b in c using the $\wedge$ operation?