CS579: Foundations of Cryptography (Spring 2019)
Homework #1

Instructor: Nikos Triandopoulos

April 3, 2019

Instructions

Please carefully read the following guidelines on how to complete and submit your solutions.

1. The homework is due on **Sunday, April 14, 2019, at 11:59pm**. Late submissions are accepted subject to the policy specified in the course syllabus. Starting early always helps!
2. Solutions are accepted only via Canvas, where your answers should be typed (preferably using LaTeX) and submitted as a .pdf file.
3. You are bound by the Stevens Honor System. Collaboration is **not** allowed for this homework. You may use any sources related to course materials, but information from external sources must be properly cited. Your submission acknowledges that you have abided by this policy.
4. This assignment provides a 10% **extra credit** opportunity!

```
JGRMQOYGHMVBJWRWQFPWHGFFDQGFPFZRKBEEBJIZQQOCIBZKLFAFGQVFZFWWE
OGWOPFGFHWOLPHLRLOLFDMFGQWBLWBWQOLKFWBYLBLYLFSFLJGRMQBOLWJVFP
FWQVHQWFFPQOQVFPQOCFPOGFWFJIGFQVHLHLROQVFGWJVFPFOLFHGQVQVFILE
OGQILHQFQGIQVVOSFAFGBWQVHQWIJVWJVFPFWHGFIWIHZZRQGBABHZQOCGFHX
```

Figure 1: A substitution-cipher ciphertext c.

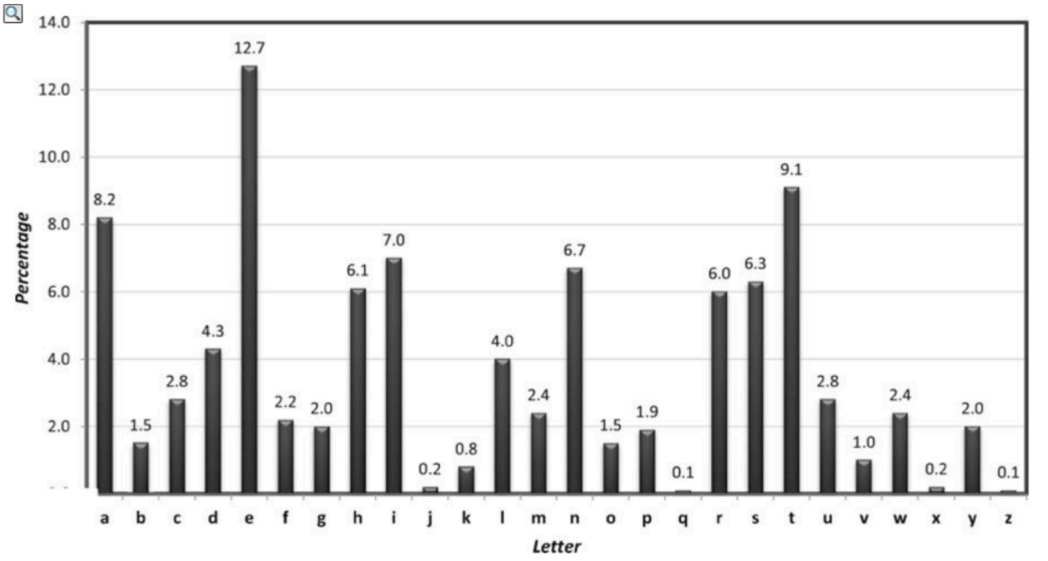

Figure 2: Histogram of English letters.

Problem 1 (40%)

(1) Provide a formal definition for the mono-alphabetic substitution cipher, or simply substitution cipher, by describing its message space $\mathcal{M}$ and the algorithms Gen, Enc and Dec.
(2) Figure 1 depicts a ciphertext c that has been produced by a substitution cipher. Use the histogram in Figure 2 to successfully decrypt c to the corresponding plaintext m. What is m?
(3) Show that the substitution cipher is trivial to break when the adversary launches a chosen-plaintext attack. How much chosen plaintext is needed to recover the entire secret key? What is the shortest chosen single-message plaintext that you can find, which is a valid English message and would successfully recover the key?
(4) Under which conditions, if any, and why, is the substitution cipher perfectly secret?

Problem 2 (20%)

(1) Consider the extension of the One-time Pad cipher, where a ciphertext c is possibly longer than the plaintext m (and the key k) by one bit, namely, by having algorithm Enc append to $m \oplus k$ a 0 or 1, with probability 0.65 or 0.3, respectively. Is this extension a perfectly secret cipher and why?
(2) Based on your answer in the previous question, prove or refute the following statement:

> An encryption scheme with message space $\mathcal{M}$ is perfectly secret if and only if, for every probability distribution $\mathcal{D}_{\mathcal{M}}$ over $\mathcal{M}$ and every $c_0, c_1 \in \mathcal{C}$, we have that:
>
> $$Pr[C = c_0] = Pr[C = c_1] \ .$$

Problem 3 (20%)

(1) Show that if $\nu_1(n)$ is a negligible function, then for any positive polynomial $p(\cdot)$, the function $\nu_2(n) = p(n) \cdot \nu_1(n)$ is also negligible. What does this imply for an attacker that attempts to break a symmetric cipher by guessing its n-bit secret key k—which is selected by algorithm Gen uniformly (at random) from all possible keys?

(2) Is $\nu(n)$ negligible, and why, if (a) $\nu(n) = \frac{n^{10^5}}{2^{n^{1/2}}}$ or (b) $\nu(n) = \frac{n^{-5^{10}}}{10^5 \cdot n^{10^5}}$.

Problem 4 (30%)

Consider an encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ that is EAV-secure according to the definition that has been discussed in class.

(1) What does the condition $|m_0| = |m_1|$ capture? Does it weaken or strengthen Π's security?

(2) Consider the notion of $\mathsf{EAV2}$-security that we get if we remove the above condition $|m_0| = |m_1|$, that is, where in the corresponding security game the adversary $\mathcal{A}$ is allowed to choose challenge messages of arbitrary length for breaking an encryption scheme $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ for arbitrary long massages. Intuitively, Π' is $\mathsf{EAV2}$-secure, if no efficient $\mathcal{A}$ can determine c_b non-negligibly better than guessing, even when $|m_0| \neq |m_1|$. Show that no $\mathsf{EAV2}$-secure scheme Π' exists.

> *Hint*: First, note that Π' is defined over message space $\mathcal{M} = \{0,1\}^*$, i.e., messages of arbitrary length. Then, assume that polynomial $p(\cdot)$ is an upper bound on the time spent by Enc' for encrypting a single bit, and consider what happens when $\mathcal{A}$ chooses $m_0 \in \{0,1\}$ and a random $m_1 \in \{0,1\}^{p(n)+c}$, where $c \geq 1$ a positive integer.

(3) Show that $\mathsf{EAV2}$-security can be achieved by encryption schemes defined over messages up to a given maximum length, i.e., by schemes Π' such that for $k \in \{0,1\}^n$, algorithm Enc' is defined over message space $\mathcal{M}' = \{m : |m| \leq \ell\}$, where $\ell \triangleq \ell(n)$ for some given polynomial $\ell(\cdot)$.

> *Hint*: Construct a scheme $\Pi' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ that encrypts messages in $\mathcal{M}'$ by employing a EAV-secure scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$. Consider an algorithm Enc' that on input message $m' \in \mathcal{M}'$, merely applies Enc on a unique and inversible encoding $m = E(m') \in \mathcal{M}$ of m' in a way that "compensates" for the absence of the restriction $|m_0| = |m_1|$ in the original game used to define EAV-security. Then, prove that Π' is $\mathsf{EAV2}$-secure via a proof by reduction.