Cryptography
Review for Test 1

1. Examples of cryptosystems:
   - **Shift**: $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_n$, $e_K(x) = x + K, d_K(y) = y - K$, $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}| = n$
   - **Affine**: $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, $K = \{(a, b) | a, b \in \mathbb{Z}_n, \gcd(a, n) = 1\}$, $e_K(x) = ax + b, d_K(y) = a^{-1}(y - b)$, $|\mathcal{P}| = |\mathcal{C}| = n, |\mathcal{K}| = \phi(n)n$ (In particular $\phi(26) = 12$)
   - **Substitution**: $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, $K$ - all permutations of $\mathbb{Z}_n$, $e_{\pi}(x) = \pi(x), d_{\pi}(y) = \pi^{-1}(y)$, $|\mathcal{P}| = |\mathcal{C}| = n, |\mathcal{K}| = n!$
   - **Vigenere**: $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_n)^m$, $e_K(x) = x + K, d_K(y) = y - K$, $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}| = n^m$
   - **Hill**: $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_n)^m$, $K$ - set of $m \times m$ invertible matrices over $\mathbb{Z}_n$, $e_K(x) = xK, d_K(y) = yK^{-1}$, $|\mathcal{P}| = |\mathcal{C}| = n^m, |\mathcal{K}| \leq n^{m^2}$ (when $n$ is prime, $\Pi_{i=0}^{m-1}(p^m - p^i)$)

2. Friedman’s Test:
   - The index of coincidence $I_c(x) = \sum \frac{f_i(f_i-1)}{n(n-1)} \approx \sum p_i^2$.
   - Explain how can the test be used to guess the length of a key in Vigenere Cipher.
   - $M_g = \sum \frac{p_i f_i}{n'}$, $n' = n/m$. How can it be used to guess a key in Vigenere Cipher.

3. Basic Probability:
   - Conditional probability.
   - Bayes’ Theorem.

4. Perfect Secrecy:
   - Check if a cryptosystem has perfect secrecy (compute conditional probabilities).
   - Shift, Affine (check directly that they have perfect secrecy).
   - Characterization of cryptosystems with perfect secrecy (when $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$) (with a proof).
• **One-time pad**: $\mathcal{P} = \mathcal{C} = \mathcal{K} = (Z_2)^n$, $e_K(x) = x + K, d_K(y) = y + K$, $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}| = 2^n$

5. **Entropy function:**

- Entropy function and conditional entropies.
- Find entropies of random variables.
- Find $H(P), H(C), H(K|C), H(P|C)$ in a given cryptosystem.
- Properties of the entropy function.
- Formula for the equivocation: $H(K|C) = H(K) + H(P) − H(C)$ (with a proof)
- Unicity distance, and the average number of spurious keys.