

Cryptography Review for Final

1. Examples of cryptosystems:

- **Shift:** $\mathcal{P} = \mathcal{C} = \mathcal{K} = Z_n$, $e_K(x) = x + K$, $d_K(y) = y - K$, $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}| = n$
- **Affine:** $\mathcal{P} = \mathcal{C} = Z_n$, $\mathcal{K} = \{(a, b) | a, b \in Z_n, \gcd(a, n) = 1\}$, $e_K(x) = ax + b$, $d_K(y) = a^{-1}(y - b)$, $|\mathcal{P}| = |\mathcal{C}| = n$, $|\mathcal{K}| = \phi(n)n$ (In particular $\phi(26) = 12$)
- **Substitution:** $\mathcal{P} = \mathcal{C} = Z_n$, \mathcal{K} - all permutations of Z_n , $e_\pi(x) = \pi(x)$, $d_\pi(y) = \pi^{-1}(y)$, $|\mathcal{P}| = |\mathcal{C}| = n$, $|\mathcal{K}| = n!$
- **Vigenere:** $\mathcal{P} = \mathcal{C} = \mathcal{K} = (Z_n)^m$, $e_K(x) = x + K$, $d_K(y) = y - K$, $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}| = n^m$
- **Hill:** $\mathcal{P} = \mathcal{C} = (Z_n)^m$, \mathcal{K} - set of $m \times m$ invertible matrices over 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, $\prod_{i=0}^{m-1} (n^m - n^i)$)

2. Friedman's Test:

- The index of coincidence $I_c(x) = \sum \frac{f_i(f_i-1)}{n(n-1)} \approx \sum p_i^2$ and how to use it to attack Vigenere Cipher.
- $M_g = \sum \frac{p_i f_{i+g}}{n'}$, $n' = n/m$ and how to use it 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)

6. Euclidean Algorithm and Chinese Remainder Theorem

- Extended Euclidean Algorithm: $r_i = s_i a + t_i b$ and $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$ and $s_i = s_{i-2} - q_{i-1} s_{i-1}$, $t_i = t_{i-2} - q_{i-1} t_{i-1}$.
- Finding the inverse of a in Z_n
- Solving system of congruences $x_i \equiv a_i \pmod{m_i}$ by $x = \sum_i a_i M_i y_i \pmod{M}$ where $M = \prod m_i$, $M_i = M/m_i$, $y_i = M_i^{-1} \pmod{m_i}$.
- Why is the solution to the system unique?

7. Facts and concepts from number theory and RSA

- Lagrange Theorem, Fermat Theorem. (with proofs)
- Order of an element in a group, primitive element, quadratic residue.
- When $b = \alpha^i$ is primitive if α is primitive? How to check if α is primitive? How to find a primitive element in Z_p^* (Theorem 5.8).
- RSA including the fact that e_K and d_K are inverses of one another (with a proof)

8. Primality testing

- Legendre and Jacobi symbols.
- Euler's Theorem. (with a proof)
- Solovay-Strassen Algorithm and the fact that if p is prime then the algorithm returns "prime". (with a proof)

- Miller-Rabin Algorithm and the fact that if p is prime then the algorithm returns "prime". (**with a proof**)

9. Pollard Algorithms

- $p - 1$ factoring algorithm. Under what assumptions and why will it work?

10. Discrete Logarithm Problem

- ElGamal Public-key cryptosystem: $\mathcal{P} = Z_p^*$, $\mathcal{C} = Z_p^* \times Z_p^*$, $\mathcal{K} = \{(p, \alpha, k, \beta) | \beta = \alpha^k, e_K(x, r) = (y_1, y_2) \text{ with } y_1 = \alpha^r, y_2 = x\beta^r, d_K(y_1, y_2) = y_2(y_1^k)^{-1}\}$.

11. Finite fields

- Irreducible polynomials and division of polynomials mod $f(x)$.
- Construction of finite fields.

12. Elliptic curves over reals and Z_p

- $\lambda = (y_2 - y_1)(x_2 - x_1)^{-1}$ when $x_1 \neq x_2$ and $\lambda = (3x_1^2 + a)(2y_1)^{-1}$ when $x_1 = x_2$ and $y_1 \neq 0$.
- $x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda(x_1 - x_3) - y_1$ or $(x_3, y_3) = \mathcal{O}$ if $x_1 = x_2, y_1 = -y_2$.