

DARTMOUTH COLLEGE DEPARTMENT OF MATHEMATICS
Math 75 Cryptography
Spring 2020

Problem Set # 3 (upload to Canvas by Friday, April 24, 11:30 am EDT)

Problems:

1. Consider the affine cipher with $\mathcal{P} = \mathcal{C} = \mathbb{Z}/n\mathbb{Z}$.

- (a) Suppose $n = 541$ and we take the key $(a, b) = (34, 71)$. Encrypt the plaintext $m = 204$, and decrypt the ciphertext $c = 431$.
- (b) Eve intercepts a ciphertext from Alice and through espionage she learns that the letter $x \in \mathcal{P}$ is encrypted as $y \in \mathcal{C}$ in this message. Show that Eve can decrypt the message using $O(n)$ trials.
- (c) Now suppose that (contrary to Kerckhoffs's principle) the integer n is not public knowledge. Is the affine cipher still vulnerable if Eve manages to steal a plaintext/ciphertext pair? How might Eve break the system?

2. Encrypt the message

Why is a raven like a writing desk

using the Vigenère cipher with keyword `rabbithole`.

3. Decrypt the following message, which was encrypted using a Vigenère cipher.

```
mgodt beida psgls akowu hxukc iawlr csoyh prtrt udrqh cengx
uuqtu habxw dgkie ktsnp sekld zlvnh wefss glzrn peao y lbyig
uaafv eqgjo ewabz saawl rzjpv feyky gylwu btlyd kroec bpfvt
psgki puxfb uxfuq cvymy okagl sactt uwlr x psgiy ytpsf rjfuw
igxhr oyazd rakce dxeyr pdobr buehr uwcue ekfic zehrq ijezr
xsyor tcylf egcy
```

- (a) Use the method of displacement coincidences to guess the key length.
- (b) Use the Kasiski test to give more evidence for your guess for the key length.
- (c) Use frequency analysis with the guessed key length to decrypt the message.

[You are encouraged to use a computer.]

4. Consider the quadratic map

$$E : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$$
$$x \mapsto x^2 + ax + b$$

with $a, b \in \mathbb{Z}/n\mathbb{Z}$. Show that if $n \neq 2$, then E is *never* an encryption function (i.e., E cannot be inverted). What can you say about other maps $x \mapsto f(x)$ where $f(x) \in \mathbb{Z}[x]$, in particular, are any polynomial maps of higher degree invertible?

5. Let $D_n = \{x \in \mathbb{R}^n : \sum_{i=1}^n x_i^2 = 1\}$ be the unit sphere in \mathbb{R}^n . Fix $x \in D_n$ and consider the function $\psi_x : D_n \rightarrow \mathbb{R}$ defined by

$$\psi_x(y) = x \cdot y = \sum_{i=1}^n x_i y_i.$$

Show that the function ψ_x achieves a unique maximum at $x = y$. How does this relate to frequency analysis?

6. Let $n, k \in \mathbb{Z}_{>0}$ and recall the general linear group $\text{GL}_k(\mathbb{Z}/n\mathbb{Z})$.

- (a) Write down all the elements of $\text{GL}_2(\mathbb{Z}/2\mathbb{Z})$. What more commonly known group is this isomorphic to?
- (b) If $n = p$ is a prime number, prove that $\text{GL}_k(\mathbb{Z}/p\mathbb{Z})$ has $(p^k - 1)(p^k - p) \cdots (p^k - p^{k-1})$ elements. [Use linear algebra over the field $\mathbb{Z}/p\mathbb{Z}$ and think of building your matrix one column at a time.]
- (c) Prove that if n, m are relatively prime positive integers, then

$$\#\text{GL}_k(\mathbb{Z}/nm\mathbb{Z}) = \#\text{GL}_k(\mathbb{Z}/n\mathbb{Z}) \cdot \#\text{GL}_k(\mathbb{Z}/m\mathbb{Z}).$$

The following subparts will provide a guide to an algebraic proof of this fact (not all of these require a proof, they are a kind of series of hints to guide your work).

- (iii) For n, m relatively prime, the map $\phi : \mathbb{Z}/nm\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, defined by $a \mapsto (a \bmod n, a \bmod m)$, is an isomorphism of groups. We can write $\phi(a) = (\phi_n(a), \phi_m(a))$ where $\phi_n : \mathbb{Z}/nm\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ is the reduction modulo n homomorphism and similarly for ϕ_m . In fact, ϕ is an isomorphism of rings with 1, i.e., respects multiplication and the multiplicative identity.
- (iii) Promote ϕ to an isomorphism $\Phi : M_k(\mathbb{Z}/nm\mathbb{Z}) \rightarrow M_k(\mathbb{Z}/n\mathbb{Z}) \times M_k(\mathbb{Z}/m\mathbb{Z})$ of rings with 1 by sending a matrix $A = (a_{ij})_{1 \leq i, j \leq k}$ to the pair $(\Phi_n(A), \Phi_m(A))$, where $\Phi_n(A) = (\phi_n(a_{ij}))_{1 \leq i, j \leq k}$ is the result of reducing all entries of A modulo n , and similarly for $\Phi_m(A)$. First you have to prove that Φ is a ring homomorphism, then that it is injective and surjective, which relies crucially on the injectivity and surjectivity of ϕ .
- (iii) Prove that $\phi(\det(A)) = (\det(\Phi_n(A)), \det(\Phi_m(A)))$ for all $A \in M_k(\mathbb{Z}/nm\mathbb{Z})$. Colloquially, this says that ϕ and Φ “respect” the determinant.
- (iii) Prove that $A \in M_k(\mathbb{Z}/nm\mathbb{Z})$ is invertible if and only if $\Phi(A)$ is an invertible element of the ring $M_k(\mathbb{Z}/n\mathbb{Z}) \times M_k(\mathbb{Z}/m\mathbb{Z})$ if and only if both $\Phi_n(A) \in M_k(\mathbb{Z}/n\mathbb{Z})$ and $\Phi_m(A) \in M_k(\mathbb{Z}/m\mathbb{Z})$ are invertible. Conclude that Φ induces a group isomorphism $\text{GL}_k(\mathbb{Z}/nm\mathbb{Z}) \cong \text{GL}_k(\mathbb{Z}/n\mathbb{Z}) \times \text{GL}_k(\mathbb{Z}/m\mathbb{Z})$ and as a consequence, we get the desired formula.
- (d) Recall the affine cipher with $\mathcal{P} = \mathcal{C} = (\mathbb{Z}/n\mathbb{Z})^k$ and with key $A \in \text{GL}_k(\mathbb{Z}/n\mathbb{Z})$. If Eve discovers the encryption of k plaintext elements, prove that the probability that she can solve for the key is $\#\text{GL}_k(\mathbb{Z}/n\mathbb{Z})/n^{k^2}$. Compute this probability for $n = 26$ and $k = 2, 3, 4$. [This was done a bit too quickly in lecture, so now you can see the details for yourself.]