CRIPTOGRAFIA ATRAVÉS DO USO DE ISOMORFISMOS

Luis Eduardo Misquita Freitas

Universidade Federal do Tocantins, luis.misquita@mail.uft.edu.br

Resumo: Esse artigo reúne conceitos de transformações lineares cuja finalidade é a de apresentar, e exemplificar a utilização de transformações lineares de espaços vetoriais na área da criptografia. Começaremos com os conceitos básicos da transformação linear no plano $\mathbb{R}^2$, logo em seguida veremos definições de núcleo, imagem, se a transformação é injetora e/ou sobrejetora. É finalmente abordando o isomorfismo, que são transformações bijetoras que possuem uma inversa T^{-1}, e então será feito uma aplicaçãoprática e real de como o isomorfismo pode ser usado para criptografar uma mensagem.

Palavras Chave: Criptografia, Transformações lineares, Isomorfismo

Introdução: A criptografia tem origem etimológica de duas palavras gregas, “Kryptós” e “Gráphein”, que significam “oculto” e “escrever” respectivamente. Portanto, a palavra “criptografia” se refere a uma maneira de se ocultar o que está escrito.

Álgebra Linear é uma das disciplinas presentes na matemática que trabalhacom matrizes, vetores, transformações lineares. Os exemplos de utilização dos modelos lineares: Pesquisas na medicina, as quais usam de transformações lineares durante testes paraefetuar previsões quanto aos efeitos e resultados de medicações.

O conceito de criptografia é ter uma mensagem de um lado, que ao ser modificada seguindo um padrão escolhido por quem codifica (chave), se torna um código indecifrável por alguémque não tenha conhecimento de qual chave foi utilizada, mas que possa ser decifrado de volta utilizando a reversão do código que gerou a chave.

Então os algoritmos criptográficos podem ser estabelecidos de diversas formas, mas nesse caso, demonstraremos aqui a criptografia feita por via das transformações lineares isomórficas. Visto que essa “reversão”feita na chave pode ser realizada utilizando o Teorema da Transformação Linear Inversa, onde se $T: V \to W$ é uma Transformação Linear e um Isomorfismo, sua inversa T^{-1} :W → V, portará os mesmos atributos.

Fundamentação Teórica: Na área da criptografia,iremos falar um pouco da teoria de espaços lineares sobre $\mathbb{R}$.

Imagine que temos a seguinte função ou aplicação T: V→W, onde V e W são espaços vetoriais em um corpo K. Logo essa função será uma transformação linear se ∀ u, v ∈ V e para todo α ∈ K, estarão presentes as seguintes proposições:

i) $T(u + v) = T(u) + T(v)$

ii) $T(\alpha * v) = \alpha * T(v)$

Se os espaços V e W forem iguais essa transformação linear irá se chama de operador linear.

Exemplo:

Ex. 1: Seja em $\mathbb{R}^2$ a função T definida por $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ e $T(x, y) = (2x - y, 0)$

Resposta: Nesse caso será necessário fazer a verificação de se $T(u + v) = T(u) + T(v)$, para isso definiremosu = (x', x'') e v= (y', y'').

$T(\alpha u + \beta v) = T(\alpha (x', x'') + \beta (y', y''))$

$= T(\alpha x' + \beta y', \alpha x'' + \beta y'')$

$= (2(\alpha x' + \beta y') - (\alpha x'' + \beta y''), 0)$

$= (2\alpha x' - \alpha x'' + 2\beta y' - \beta y'', 0)$

$= (2\alpha x' - \alpha x'', 0) + (2\beta y' - \beta y'', 0)$

$= \alpha (2x' - x'', 0) + \beta (2y' - y'', 0)$

$= \alpha T(u) + \beta T(v)$

Agora verificando se $T(\alpha u) = \alpha T(u)$

$T(\alpha u) = T(\alpha x', \alpha y') = (2\alpha x' - \alpha y', 0)$

$= (2\alpha x' - \alpha y', 0)$

$= \alpha (2x' - y', 0)$

$= \alpha * T(u)$

Portanto T é uma transformação linear.

1. Definição do núcleo de uma transformação linear: Sendo assim V e W sendo espaços vetoriais sobre um corpo $\mathbb{R}$ e T : U → V isso acaba sendo uma transformação linearde V em W,o núcleo de T é simbolizado por Ker (T), ou ainda N (T), é o subconjuntodo domínio e formado pelos vetores que são levados ao vetor nulo do contradomínio.

   N (T) = {v ∈ V | T (v) = 0}

Ex. 2: Considerando uma função T: $\mathbb{R}^2$ → $\mathbb{R}^2$ definida por T: (x, y) ; (2x+ y, 3x + 2y) determineuma base para o núcleo de T.

Resposta:

T (x, y) = (0, 0) ↔ (2x + y, 3x + 2y) = (0, 0)

$$\begin{cases} 2x + y = 0 \\ 3x + 2y = 0 \end{cases}$$

y = -2x

3x + 2 (-2x) = 0 → 3x - 4x = 0 → -x = 0 → x = 0

y = -2 * 0 → y = 0

Conclui-se que x = y = 0. Então N (T) = {(0, 0)}

2. Definição da imagem de uma transformação linear: Sejam U e V espaços vetoriais sobre $\mathbb{R}$ e T: U V uma Transformação Linear, indica-se por Im(T) e denomina-se imagem de T, o seguinte subconjunto de V:

   Im(T) = {T(u) / u ∈ U}

Ex. 3: Considere T: $\mathbb{R}^2$ → $\mathbb{R}^2$ tal que T(x,y) = (x – 2y, y), encontre o Im(T).

Resposta:

Im(T) = {T(x,y)/(x,y) ∈ $\mathbb{R}^2$}

Im(T) = {(x –2y, y) / x, y ∈ $\mathbb{R}^2$}

Im(T) = [(1) + (-2, 1)], pois:

(x –2y, y) = (x) + (-2y, y)

(x –2y, y) = x (1) + y (-2, 1).

3. Definição de transformação linear injetora: Imagine uma Transformação Linear T: U→ V, então podemaos dizemos que T é injetora se dados u1 ∈ U, u2 ∈ U com T(u1) = T(u2) tivermos u1 = u2, ou equivalentemente, T é injetora se dados u1, u2 ∈ U com u1 = u2, então T(u1) ≠ T(u2).

Ex. 4: Suponhamos que Ker(T)= {0} e dados u1 e u2 U, então:

T(u1) = T(u2) → T(u1) - T(u2) = 0 →

T (u1 - u2) = 0 → u1 - u2 ∈ Ker(T) →

u1 - u2 = 0 → u1 = u2

O que mostra que T é injetora.

4. Definição de transformação linear sobrejetora: imagine que e Dada uma Transformação Linear T: U→ V, T é sobrejetora se a imagem de T coincidir com V (o contradomínio), ou seja, T(U) = V.

5. Definição de transformação linear bijetora e isomorfismo: Consideramos Isomorfismo do espaço vetorial U no espaço vetorial V (ambos sobre $\mathbb{R}$) uma Transformação Linear T: U→ V que seja bijetora

"Chama-se isomorfismo do espaço vetorial V no espaço vetorial W a umatransformação linear T: V→ W, que é bijetora. Neste caso, os espaços vetoriais V e W sãoditos isomorfos. Sendo que todo espaço vetorial V de dimensão n é isomorfo a $\mathbb{R}n$, assim, dois espaços vetoriais de dimensão finita são isomorfos se tiverem a mesma dimensão." (STEINBRUSCH, 1987, p.181)

EX. 5: Seja a Transformação Linear T: 2 2 definida por: (x, y) (2x – y, x+ y) é um Isomorfismo.

Resposta:

i) T ((x1, y1) +(x2, y2)) = T (x1 + x2, y1 + y2) = (2(x1 + x2) – (y1 + y2), (x1 + x2) +(y1 + y2))

= (2x1 + 2x2 -y1 - y2, x1 + x2+ y1 + y2)

= ((2x1 – y1) + (2x2 – y2), (x1+ y1) + (x2+ y2))

= T (x1, y1) +T (x2, y2)

ii) T ((x1, y1)) = T (x1, y1) = (2(x1) +(y1), (x1) +(y1))

= ((2x1 – y1), (x1+ y1))

= T (x1, y1)

iii) T (x1, y1) = T (x2, y2) → (2x1 – y1, x1+ y1) = (2x2 – y2, x2+ y2)

$$\begin{cases} 2x1 - y1 = 2x2 - y2 \\ x1 + y1 = x2 + y2 \end{cases}$$

→ x1 = x2 e y1 = y2, logo T é Injetora.

iv) Dado (x, y) pertencente ao contradomínio, existe (a, b) pertencente ao domínio, tal que, T (a, b) = (x, y). De fato:

Basta tomar (x, y) = (a + b/3, 2b –a/3) para que se tenha T (a, b) = T (x, y). Logo, T é sobrejetora.

i) e ii) garante que T é uma Transformação Linear.

iii) e iv) prova que T é Isomorfismo.

6. Definição de transformação linear inversa: Se T:U V for uma Transformação Linear e um Isomorfismo, sua inversa T-1: V → U, também será uma Transformação Linear e um Isomorfismo.

Ex. 6: Como T é um Isomorfismo, temos que T é bijetora, logo existe sua inversa T-1

Resposta:

i) Dados v1 e v2 em V, como T é sobrejetora, temos que:

T(u1) = v1 e T(u2) = v2, logo,

T -1(v1 + v2) = T-1(T(u1) + T(u2)) = T-1(T (u1 + u2)) = u1 + u2 = T-1(v1) + T-1(v2)

Pois, T-1(T(u1)) =T-1(v1) u1 = T-1(v1) e T-1(T(u2)) =T-1(v2) u2 = T-1(v2)

ii) Dados v1 V ∈ $\mathbb{V}$ e a ∈ $\mathbb{R}$, como T é sobrejetora, temos que:

T(u1) = v1, logo,

T-1(av1) = T-1(aT(u1)) = T-1(T(u1)) = au1 = aT -1(v1)

iii) Como T-1(T(u)) = u os vetores Ker(T-1) são os vetores T(u) = 0,

mas, como T é injetora, u = 0.

Logo, Ker(T-1) = {0}

T -1 também é injetora.

iv) Como T é sobrejetora, para todo v V, existe u U, tal que T(u) = v. Então, T-1(T(u)) = u T-1(v) = u

Assim para todo u U, existe v V, tal que T-1(v) = u.

Logo, T-1 também é sobrejetora.

Por i) e ii) garantimos que T-1 é uma Transformação Linear.

Por iii) e iv) provamos que T-1 é Isomorfismo.

RESULTADOS E DISCUSSÃO: Agora que os conceitos necessários foram visados, irei demonstrar como o isomorfismo podeser aplicado na codificação de uma mensagem comum, a fim de demonstrar de forma didática, a utilização desse mecanismo.

Agora, colocando na prática, iniciaremos representando abaixo uma tabela para asubstituição das letras do alfabeto por valores numéricos aleatórios, levando em consideração apenas as letras presentes e o espaço entre elas.

Tabela 01. Tabela de Conversão

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
4	17	11	10	14	15	-2	-11	8	6	1	13	-4	12
O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**SPC**	
-10	3	5	-7	0	9	2	-3	-5	18	20	-9	-6	

Agora que definimos a tabela vamos usa a seguinte frase pra ser codificada:

TUDO SE TRANSFORMA

Tabela 02. Substituição de cada letra por seu código

T	**U**	**D**	**O**	**SPC**	**S**	**E**	**SPC**	**T**
9	2	10	-10	-6	0	14	-6	9
R	**A**	**N**	**S**	**F**	**O**	**R**	**M**	**A**
-7	4	12	0	15	-10	-7	-4	4

no uso das transformações lineares , a regra de transformaçãousada será do espaço

$$T(x, y) = (2x + y, 3x + 2y)$$

$\mathbb{R}^2$:

Então, como nossa transformação é do espaço $\mathbb{R}^2$, a transformação será aplicada a cada par de caracteres da mensagem.

T (9, 2) = (2 * 9 + 2, 3 * 9 + 2 * 2) = **(20, 31)**
T (10, -10) = (2*10 + (-10), 3 * 10 + 2 * (-10)) = **(10, 10)**
T (-6, 0) = (2 * (-6) + 0, 3 * (-6) + 2 * 0) = **(-12, -18)**
T (14, -6) = (2 * 14 + (-6), 3 * 14 + 2 (-6)) = **(22, 30)**
T (9, -7) = (2 * 9 + (-7), 3 * 9 + 2 * (-7)) = **(11, 13)**
T (4, 12) = (2 * 4 + 12, 3 * 4 + 2 *12) = **(20, 36)**
T (0, 15) = (2 * 0 + 15, 3 * 0 + 2 * 15) = **(15, 30)**
T (-10, -7) = (2 * (-10) + (-7), 3 * (-10) + 2 * (-7)) = **(-27, -44)**
T (-4, 4) = (2 * (-4) + 4, 3 * (-4) + 2 * 4) = **(-4, -4)**

Após a transformação, teríamos a seguinte tabela:

Tabela 03. Pós conversão

?	**?**	**D**	**D**	**?**	**?**	**?**	**?**	**C**
20	31	10	10	-12	-18	22	30	11
L	**?**	**?**	**F**	**?**	**?**	**?**	**M**	**M**
13	20	36	15	30	-27	-44	-4	-4

Temos $T^{-1}(x, y) = (2x – y, -3x + 2y)$
Agora, só converter (em pares, lembrando que o espaço usado é $\mathbb{R}^2$):

T (20, 31) = (2 * 20 – 31, -3 * 20 + 2 *31) = (9, 2)
T (10, 10) = (2 * 10 – 10, -3 * 10 + 2 * 10) = (10, -10)
T (-12, -18) = (2 * -12 - (-18), -3 * (-12) + 2 * (-18)) = (-6, 0)
T (22, 30) = (2 * 22 – 30, -3 * 22 + 2 * 30) = (14, -6)
T (11, 13) = (2 * 11 – 13, -3 * 11 + 2 * 13) = (9, -7)
T (20, 36) = (2 * 20 – 36, -3 * 20 + 2 * 36) = (4, 12)
T (15, 30) = (2 * 15 – 30, -3 * 15 + 2 * 30) = (0, 15)
T (-27, -44) = (2* (-27) - (-44), -3 * (-27) + 2 * (-44) = (-10, -7)
T (-4, -4) = (2 * (-4) - (-4), -3 * (-4) + 2 * (-4)) = (-4, 4)

Após aplicar a mensagem cifrada em T^{-1} a pessoa que recebeu a mensagem obterá oseguinte código:

9 2 10 -10 -6 0 14 -6 9 -7 4 12 0 15 -10 -7 -4 4

Código o qual é igual ao da primeira cifragem, presente na tabela 01. Após conferir atabela, o remetente chega ao texto de origem:

TUDO SE TRANSFORMA

CONSIDERAÇÕES FINAIS: Após todo o processo apresentado, é perceptível a usabilidade das transformações lineares para criptografar mensagens. Apesar de o algoritmo usado ser pouco complexo, sua eficiência é mais que suficiente para a codificação de coisas simples como mensagens, além deque o processo pode se tornar cada vez mais seguro, através de mais rodadas de codificação seguindo a regra de transformação por mais vezes.

REFERÊNCIAS BIBLIOGRÁFICAS:

http://dspace.nead.ufsj.edu.br/trabalhospublicos/bitstream/handle/123456789/68/EDUARDO%20SCHWARTZ_12293_assignsubmission_file_TCC-Transformações%20Lineares.pdf

https://www.ieeeuel.org/post/criptografia-origem-e-história

https://www.ime.unicamp.br/~marcia/AlgebraLinear/isomorfismo_automorfismo.html

https://imef.furg.br/images/stories/Monografias/Matematica_aplicada/2019/2019-2HellenTrindade.pdf

https://repositorio.ufsc.br/bitstream/handle/123456789/119888/Lucio_Helio.pdf?sequence=1&isAllowed=y

https://moodle.ufsc.br/pluginfile.php/1310280/mod_resource/content/1/aula8.pdf