مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۴۷ -۴۵

روش جدید تولید ماتریس کلید و وارون آن برای الگوریتم رمز هیل

سعید محمدیان سمنانی*

استادیار دانشگاه سمنان

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

الگوریتم رمز هیل کاربرد جبر خطی در رمزنگاری است که علمی در کد و دی‌کدکردن پیام‌های متنی است، این رمزنگاری مستلزم استفاده از یک ماتریس$n\times n$ غیرمنفرد با عناصر صحیح است که آن را ماتریس کلید می‌نامیم. این‌گونه ماتریس ها خواصی دارند که در این مقاله قصد داریم تا روش جدیدی برای معرفی آن‌ها و وارون آن‌ها پرداخته و سپس به کمک آن‌ها عبارتی را کدگذاری و سپس آن را دی‌کد نمائیم.

واژه‌های کلیدی: ماتریس کلید، کدگذاری، دی‌کد، رمز هیل

۱- مقدمه

در دنیای امروز حفاظت اطلاعات مبحثی است که از اهمیت بسیار بالایی برخوردار است که این اهمیت شاید در روزگاران پیشین به این نبوده است. علم کدگذاری و رمزگشایی یکی از علوم بسیار مهم و استراتژیک یک به خصوص در صنعت تلفن‌های همراه، ارتباطات، بازرگانی، الکترونیک و ارسال ایمیل‌های خصوصی است.یکی از روش‌های کدگذاری‌کردن اطلاعات استفاده از روش رمز هیل[1] است [۳-۲].

رمز هیل روشی برای ارسال یک پیام متنی به متنی جدید است که قابل فهمبرای هیچ کس دیگری نیست مگر آن‌که شخص با قاعده رمزگشایی آن آشنا باشد. در واقع Hill-K-Cipher به قرار زیر عمل می‌کند. ابتدا به کاراکترهای موجود در ادبیات زبانی که با آن روش Hill-cipher به کار می‌رود اعدادی نسبت داده می‌شود.مثلاً اگر k کاراکتر در ادبیات این زبان استفاده شود به هرکدام از آن‌ها عدد منحصر به فرد ۰، ۱، ۲، ..... k-1 نسبت داده می‌شود. همان‌طورکه گفته شد این K کاراکتر می‌توانند حروف الفبا و علائم نوشتاری از قبیل علامت سوال (؟)، حروف فاصله (-)، کاما (،) و غیره باشند.

در این روش، برای رمزگشایی متنی که کدگذاری شده به یک ماتریس به نام ماتریس کلید A و وارون آن A^{-1} نیازمندیم بدیهی است که ماتریس کلید باید غیرمنفرد باشد و نیز خواص دیگری باید داشته باشد که به آن‌ها اشاره می‌کنیم.

در این مقاله روشی ساده برای معرفی ماتریس A و وارون آن ارائه خواهیم کرد.

۲- روش تحقیق

فرض کنیم $\alpha_k \dots, \alpha_2, \alpha_1$ تمامی کاراکترهایی باشند که در یک زبان به کار می‌روند به هر کدام از این کاراکترها اعداد ۰، ۱، ۲، ..... k-1 را به ترتیب نسبت می‌دهیم (البته می‌توان اعداد را به طور نامنظم و یا به پیمانه خاصی و .... نسبت داد).

اکنون فرض کنیم که $P = \alpha_1\alpha_2 \dots \alpha_l$ یک متن ۱ کاراکتری باشد که در آن، $1 \le l \le k$ می‌باشد.

ابتدا این متن را به یک رشته عددی به صورت زیر متناظر می‌کنیم:

$$P = 0,1,2, \dots, l-1$$

اکنون P را به صورت بردار ستونی $P_1, P_2, \dots, P_m$ می‌نویسیم که هرکدام از این بردارها دارای r سطر باشند. (r عددی دلخواه صحیح و مثبت است)

$$P_1 = [0,1,2, \dots, r-1]^t, P_2 = [r, r+1, \dots, 2r-1]^t, \dots$$

$$, P_m = [(m-1)r, (m-1)r+1, \dots l-1]^t$$

تذکر: چنان‌چه برای P_m کم‌تر از r مولفه باقی بماند، به عبارتی

*رایانامه نویسنده مسئول: s_mohammadian@Semanan.ac.ir

1- Hill Cipher

اگر r عدد l را عاد نکند(یعنی r بر l بخشپذیر نباشد) آن‌گاه عدد آخر را آن‌قدر تکرار می‌کنیم تا تعداد مولفه های P_m نیز r تا گردد.

در گام بعد باید ماتریسی مانند $A = [a_{ij}]_{r\times r}$ بیابیم به نام ماتریس کلید و آن‌را از چپ در P ضرب می‌کنیم.

$$\mathrm{Ap} = [AP_1, AP_2, \dots, AP_m] \quad (mod\ k)$$

ماتریس AP را ماتریس Hill r-cipher می‌نامیم. به عبارت دیگر، متن P توسط الگوریتم رمز هیل کدگذاری شده است و به منظور رمزگشایی AP ما نیازمند معکوس ماتریس کلید یعنی A^{-1} هستیم. با توجهبه آن‌که $A^{-1} = \frac{1}{|A|}adj(A)$ و از آن‌جایی‌که درایه‌های A^{-1} باید صحیح و متعلق به $\{0,1,2,\dots,k-1\}$ باشند به عبارت دیگر، چون درایه‌های A همگی صحیح و مثبت هستند لذا کافی است که $\frac{1}{|A|}$ را به پیمانه K محاسبه کنیم ابتدا به یک تعریف و یک قضیه اشاره می‌کنیم.

تعریف: اگر a عددی صحیح و غیرصفر باشد کوچک‌ترین عدد صحیح و مثبت x که در رابطه (ax≡ ۱ mod k) صدق کند وارون a به پیمانه k خوانده می‌شود. به عنوان مثال، از ۱۳x≡1(mod 32) نتیجه می‌شود که x=۵ بنابراین ۵=۱۳$^{-1}$ به پیمانه ۳۲ است.

قضیه: فرض کنیم $a, b, c \in \mathbb{Z}$ توأماً صفر نباشند آن‌گاه معادله $ax + by = c$ در Z دارای جواب است اگر و تنها اگر $d = (a, b)|c$، و اگر x_0 و y_0 یکی از جواب‌های معادله باشد آن‌گاه جواب عمومی آن را می‌توان از رابطه:

$$x = x_0 + \frac{b}{d}t$$
$$y = y_0 - \frac{a}{d}t$$

که $t \in \mathbb{Z}$ به دست آورد.

اکنون اگر a و k اعداد صحیح مفروض باشند آن‌گاه x وارون a به پیمانه k است. هرگاه $ax \equiv 1 \pmod k$ و یا به ازای $y \in \mathbb{Z}$ ax-1=ky و یا $ax - ky = 1$.

بنابر قضیه بالا، معادله اخیر دارای جواب است اگر و تنها اگر d=(a,k)|1 و یا (a,k)=1 لذا کافی است که ماتریس کلید $A = [a_{ij}]_{r\times r}$ دارای این خاصیت باشد که |A|=a و (|A|,k)=1

بدیهی است که چنین ماتریسی منحصر به فرد نیست و هر ماتریسی که دترمینان آن برای a باشد می‌تواند انتخاب گردد برای سهولت می‌توانیم ماتریس قطری در نظر بگیریم که حاصل ضرب درایه‌های روی قطر آن برابر a باشد، باید معادله $|A|x - ky = 1$ را حل کنیم و از آن‌جا:

$$x = \frac{ky + 1}{|A|} \qquad y \in \mathbb{Z}$$

با یافتن کوچک‌ترین عدد صحیح مثبت برای y و از آن‌جا:

$$\frac{1}{|A|} \equiv \mathrm{x} \pmod{\mathrm{k}}$$

سرانجام برای رمزگشایی Ap می‌توانیم از

$$A^{-1}(\mathrm{AP}) = \frac{1}{|A|}\ adj(A)(AP)$$

$$p = x\ (adj\ (A)(AP))\ (\mathrm{mod\ k})$$

استفاده کنیم.

مثال: فرض کنیم بخواهیم متن زیر را ابتدا رمزگذاری و سپس با Hill-3-cipher رمزگشایی کنیم.

P=That's life; feel it, live it & enjoy it.

a	b	c	d	...	z	&	.	⊔	;	,	.
0	1	2	3	...	25	26	27	28	29	30	31

با نمادهای بالا در این مثال داریم k=32 و l=41

t	h	a	t	,	s	⊔		i	f	e	;	⊔	f	e	e	l	⊔	i	t	,
19	7	0	19	31	18	28	11	8	5	4	29	28	5	4	4	11	28	8	19	30

$$\mathrm{P} = \begin{bmatrix} 19 & 19 & 28 & 5 & 28 & 4 & 8 & 28 & 21 & 8 & 26 & 13 & 14 & 19 \\ 7 & 31 & 11 & 4 & 5 & 11 & 19 & 11 & 4 & 19 & 28 & 9 & 28 & 27 \\ 0 & 18 & 8 & 29 & 4 & 28 & 30 & 8 & 28 & 28 & 4 & 14 & 8 & 27 \end{bmatrix}$$

با قراردادن r = 3 داریم:

$$\mathrm{P} = \begin{bmatrix} 19 & 19 & 28 & 5 & 28 & 4 & 8 & 28 & 21 & 8 & 26 & 13 & 14 & 19 \\ 7 & 31 & 11 & 4 & 5 & 11 & 19 & 11 & 4 & 19 & 28 & 9 & 28 & 27 \\ 0 & 18 & 8 & 29 & 4 & 28 & 30 & 8 & 28 & 28 & 4 & 14 & 8 & 27 \end{bmatrix}$$

حال باید ماتریس غیرمنفردی $A = [a_{ij}]_{3\times3}$ معرفی کنیم که ۱= (|A|,32) برای مثال قرار می‌دهیم |A|=15 (کاملاً اختیاری است و کافی است در شرط (|A|,32)=1 صدق کند.) و ماتریس A را به صورت زیر در نظر می‌گیریم:

$$\mathrm{A} = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$|\mathrm{A}| = 15$$

برای کدگذاری متن P داریم:

$$\mathrm{AP} = \begin{bmatrix} 25 & 25 & 20 & 15 & 20 & 12 & 24 & 20 & 31 & 24 & 14 & 7 & 8 & 25 \\ 3 & 27 & 23 & 20 & 25 & 23 & 31 & 23 & 20 & 31 & 12 & 13 & 12 & 7 \\ 0 & 18 & 8 & 29 & 4 & 28 & 30 & 8 & 28 & 28 & 4 & 14 & 8 & 27 \end{bmatrix}$$

درایه‌های AP به پیمانه ۳۲ هستند بنابراین، متن مذکور به صورت زیر کدگذاری می‌گردد:

Zda. Suxipu; uzemxuy’, uxi’ uuy’u omehnoimizh.

حال فرض کنید بخواهیم متن اخیر را دی‌کد نمائیم:

$$adj(A) = \begin{bmatrix} 5 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 15 \end{bmatrix}$$

$$|A| = 15 \rightarrow 15x \equiv 1 \ (mod\ 32) \rightarrow 15x - 32y = 1$$

$$x = 15\ , (y = 7) \rightarrow \frac{1}{|A|} = 15 \ (mod\ 32)$$

$$A^{-1} = \frac{1}{|A|} adj(A) = \begin{bmatrix} 11 & 0 & 0 \\ 0 & 13 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$A^{-1}(AP) = \begin{bmatrix} 275 & 275 & 220 & 165 & 220 & 132 & 264 & 220 & 341 & 264 & 154 & 77 & 88 & 275 \\ 39 & 351 & 299 & 260 & 325 & 299 & 403 & 299 & 260 & 403 & 156 & 169 & 156 & 91 \\ 0 & 18 & 8 & 29 & 4 & 28 & 30 & 8 & 28 & 28 & 4 & 14 & 8 & 27 \end{bmatrix}$$

چنان‌چه ماتریس اخیر را به پیمانه ۳۲ بنویسم داریم:

$$p = \begin{bmatrix} 19 & 19 & 28 & 5 & 28 & 4 & 8 & 28 & 21 & 8 & 26 & 13 & 24 & 19 \\ 7 & 31 & 11 & 4 & 5 & 11 & 19 & 11 & 4 & 19 & 28 & 9 & 28 & 27 \\ 0 & 18 & 8 & 29 & 4 & 28 & 30 & 8 & 28 & 28 & 4 & 14 & 8 & 27 \end{bmatrix}$$

۵- نتیجه گیری

در رمز نگاری می توان به گونه های متفاوت علائم یک زبان را شماره گذاری کرد. به خصوص چنانچه بخواهیم احتمال کشف رمز را توسط افراد ناشناس کمتر کنیم، می توانیم شماره گذاری علائم آن زبان را تغییر دهیم.

۶- مراجع

[1] B. Acharya, G. SankarRath, S. Kumar Patra, and S. Kumar Panigrahy, “Novel Methods of Generating Self-invertible matrix for Hill cipher Algorithm,” International Journal of security, vol. 1.

[2] M. Eisenberg, “Hill cipher and modular linear algebra,” mimeographed notes, university of Massachusettsa, vol. 19 1998.

[3] D. Kahn, “The Codebreakers, The Story of Secret Writing,” Weiden-feld and Nicolson, London, pp. 404-410, 1967.

[4] S. H. Lester, “Cryptograph in an algebraic alphabet,” Amer. Math. Monthly, vol. 36, pp. 306-312, 1929.

[5] S. H. Lester, “Concerning certain linear transformation apparatus of cryptography,” Amer. Math. Monthly, vol. 38, pp. 135-154, 1931.

[6] W. stalling, “cryptography and network security,” 4th edition, printice Hall, 2005.