به نام خداوند بخشنده مهربان

مجتمع آموزش عالی کناباد	مبانی ماتریس ها و جبرخطی	نیمسال اول ۹۳–۹۴
مدرس :فهیمه اخوان		مهلت تحویل :۹۳/۱۰/۳۰

دراین پروژه کاربرد ماتریس ها در رمزی کردن و رمز گشایی پیام های متنی به روش HILL CIPHER بررسی می شود.

۱-کُد و رمز کردن پیام های متنی

یکی از ساده ترین روش ها برای کد کردن پیام جایگزین کردن هریک از حروف با حرف دیگر با استفاده از جدولی بصورت جدول (۱)است .این روش در بسیاری از جدولها و معماهای موجود در مجلات و روزنامه ها مورد استفاده قرار میگیرد . در این روش فاصله بین کلمات و علامت های نگارشی در نظر گرفته نشده است.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Y	C	W	O	G	R	D	B	P	I	Z	X	K	L	N	M	T	S	E	F	H	J	A	V	U	Q

جدول (۱)

بطور مثال عبارتVECTOR SPACE با این روش بصورت JGWFNSEMYWG کد می شود. برای دیکد کردن این روش از جدولی بصورت جدول (۲)استفاده می نماییم.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
W	H	B	G	S	T	E	U	J	V	M	N	P	O	D	I	Z	F	R	Q	Y	X	C	L	A	K

جدول(۲)

بطور مثال عبارت کد شده XPLGYSYXDGCSY با استفاده از جدول(۲) بصورت LINEARALGEBRA دیکد می شود.یکی ازاشکالات عمده این روش کد گذاری سهولت یافتن رمز آن است.زیرا در این روش هر یک از حروف همواره با یک حرف ثابت کد می شود و با توجه به تعداد تکرار برخی از حروف پر کاربرد در زبان انگلیسی به آسانی می توان جدول کد گذاری مربوطه را بدست آورد.

یکی دیگراز روشهای کد گذاری ، که در مبحث جبر خطی مطرح می گردد، استفاده ار اعداد در کدکردن پیام های متنی است.در این روش با احتساب فاصله بین کلمات و دو علامت نگارشی نقطه و علامت پرسشی از جدولی به شکل زیر برای کد گذاری استفاده می شود.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	?	⌐
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

جدول(۳)

پیام متنی SINGULAR VALUE DECOMPOSITION با استفاده از این روش با تفکیک به بردارهای سه تایی به صورت زیر کد می شود

$$\begin{matrix} S & \begin{bmatrix}18\\8\\13\end{bmatrix} & G & \begin{bmatrix}6\\20\\11\end{bmatrix} & A & \begin{bmatrix}0\\17\\28\end{bmatrix} & V & \begin{bmatrix}21\\0\\11\end{bmatrix} & U & \begin{bmatrix}20\\4\\28\end{bmatrix} & D & \begin{bmatrix}3\\4\\2\end{bmatrix} & O & \begin{bmatrix}14\\12\\15\end{bmatrix} & O & \begin{bmatrix}14\\18\\8\end{bmatrix} & T & \begin{bmatrix}19\\8\\14\end{bmatrix} & N & \begin{bmatrix}13\\13\\13\end{bmatrix} \\ I & & U & & R & & A & & E & & E & & M & & S & & I & & N & \\ N & & L & & \neg & & L & & \neg & & C & & P & & I & & O & & N & \end{matrix}$$

لازم به ذکر است در انتهای پیام جهت تکمیل بردار نهایی می توان حرف آخر را به تعداد مورد نیاز تکرار نمود.در مورداین مثال حرفN در انتهای عبارت دو بار تکرار شده است.نهایتا پیام حاصل را می توان بصورت ماتریس زیر نمایش داد،

$$P=\begin{bmatrix}18 & 6 & 0 & 21 & 20 & 3 & 14 & 14 & 19 & 13\\ 8 & 20 & 17 & 0 & 4 & 4 & 12 & 18 & 8 & 13\\ 13 & 11 & 28 & 11 & 28 & 2 & 15 & 8 & 14 & 13\end{bmatrix}$$

تا این مرحله توانستیم پیام متنی با استفاده از جدول(۳) بصورت اعداد کد نماییم.حال برای رمزی کردن این پیام از یک ماتریس کلیدی(key matrix) معکوس پذیر ۳×۳ استفاده می نماییم،

$$A=\begin{bmatrix}3 & 10 & 20\\ 20 & 9 & 17\\ 9 & 4 & 17\end{bmatrix}$$

با ضرب ماتریس کلیدی Aدر ماتریسp پیام رمز شده بدست می آید:

$$AP=\begin{bmatrix}394 & 438 & 730 & 283 & 660 & 89 & 462 & 382 & 417 & 429\\ 653 & 487 & 629 & 607 & 912 & 130 & 643 & 578 & 690 & 598\\ 415 & 321 & 544 & 376 & 672 & 77 & 429 & 334 & 441 & 390\end{bmatrix}$$

برای بیان این ماتریس بصورت عبارت متنی رمز شده باید درایه های ماتریس را به اعدادی در محدوده 0 تا 28 تبدیل نماییم.برای این منظور از محاسبات ماجولار یا پیمانه ای (modular arithmetic) استفاده می نماییم.در این روش هریک از اعداد را با باقیمانده تقسیم آن عدد بر29 جایگزین می نماییم،بطور مثال،

$$394=29\times13+17 \quad \rightarrow \quad 394\equiv17\,(\mathrm{mod}\,29)$$
$$653=29\times22+15 \quad \rightarrow \quad 653\equiv15\,(\mathrm{mod}\,29)$$
$$415=29\times14+9 \quad \rightarrow \quad 415\equiv19\,(\mathrm{mod}\,29)$$
$$\vdots$$

به این ترتیب ماتریس رمز شده در $\mathrm{mod}\ 29$ بصورت زیر بیان می شود:

$$AP=\begin{bmatrix}17 & 3 & 5 & 22 & 22 & 2 & 27 & 5 & 11 & 23\\ 15 & 23 & 20 & 27 & 13 & 14 & 5 & 27 & 23 & 18\\ 9 & 2 & 22 & 28 & 5 & 19 & 23 & 15 & 6 & 13\end{bmatrix}$$

حال با استفاده از جدول(۳)پیام رمز شده را می نویسیم،

RPJDXCFUWW? WNFCOT?FXF?PLXGXSN

مزیتی که این روش دارد این است که پیدا کردن رمز به راحتی امکان پذیر نیست و هر حرف به چند صورت متفاوت کد شده است.بطور مثال حرف O در این پیام سه بار تکرار شده و به فرم های Gو F و? رمز شده است .

۲- رمز گشایی و دیکُد کردن پیام های رمز شده

برای رمز گشایی عبارتهای رمز شده و بازیابی پیام اصلی، از معکوس ماتریس کلیدی در mod29 استفاده می شود.برای محاسبه معکوس اعداد در mod29 به صورت زیر عمل می کنیم،

$$2\times 15 = 30 \equiv 1 \,(\mathrm{mod}\, 29) \;\rightarrow\; \frac{1}{2} \equiv 15 \,(\mathrm{mod}\, 29)$$

$$3\times 10 = 30 \equiv 1 \,(\mathrm{mod}\, 29) \;\rightarrow\; \frac{1}{3} \equiv 10 \,(\mathrm{mod}\, 29)$$

$$4\times 22 = 88 \equiv 1 \,(\mathrm{mod}\, 29) \;\rightarrow\; \frac{1}{4} \equiv 22 \,(\mathrm{mod}\, 29)$$

$$\vdots$$

در واقع برای دو عدد a و b اگر $a\times b \equiv 1 \,(\mathrm{mod}\, 29)$ باشد،در اینصورت عدد b معکوس عدد a خواهد بود.حال می خواهیم معکوس ماتریس A را بدست آوریم:

$$A = \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \;\rightarrow\; \mathrm{A}^{-1} = \frac{1}{-1635}\begin{bmatrix} 85 & -90 & -10 \\ -187 & -129 & 394 \\ -1 & 78 & -173 \end{bmatrix}$$

برای بدست آوردن A^{-1} در mod 29 بصورت زیر عمل می کنیم،

$$1635\times b \equiv 1 \,(\mathrm{mod}\, 29) \rightarrow b = 8 \rightarrow \frac{1}{1635} \equiv 8 \,(\mathrm{mod}\, 29)$$

$$A^{-1} = \begin{bmatrix} -680 & 720 & 80 \\ 1496 & 1032 & -2792 \\ 8 & -624 & 1348 \end{bmatrix} = \begin{bmatrix} 16 & 24 & 22 \\ 17 & 17 & 21 \\ 8 & 14 & 21 \end{bmatrix}$$

می توان بررسی کرد که A^{-1} بدست آمده معکوس ماتریس کلیدی A در mod29 می باشد.

$$A^{-1}A = \begin{bmatrix} 16 & 24 & 22 \\ 17 & 17 & 21 \\ 8 & 14 & 21 \end{bmatrix}\begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} = \begin{bmatrix} 726 & 464 & 1102 \\ 580 & 407 & 986 \\ 493 & 290 & 755 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} (\mathrm{mod}\, 29)$$

حال می توان از ماتریس A^{-1} برای رمز گشایی عبارت رمز شده استفاده کرد.پیام رمز شده بصورت زیر می باشد:

RPJDXCFUWW? WNFCOT?FXF?PLXGXSN

ابتدا آن را بصورت بردارهای ستونی سه تایی نمایش می دهیم،

$$\begin{matrix} R \\ P \\ J \end{bmatrix} \begin{matrix} 17 \\ 15 \\ 9 \end{bmatrix} \quad \begin{matrix} D \\ X \\ C \end{bmatrix} \begin{matrix} 3 \\ 23 \\ 2 \end{bmatrix} \quad \begin{matrix} F \\ U \\ W \end{bmatrix} \begin{matrix} 5 \\ 20 \\ 22 \end{bmatrix} \quad \begin{matrix} W \\ ? \\ \neg \end{bmatrix} \begin{matrix} 22 \\ 27 \\ 28 \end{bmatrix} \quad \begin{matrix} W \\ N \\ F \end{bmatrix} \begin{matrix} 22 \\ 13 \\ 5 \end{bmatrix} \quad \begin{matrix} C \\ O \\ T \end{bmatrix} \begin{matrix} 2 \\ 14 \\ 19 \end{bmatrix} \quad \begin{matrix} ? \\ F \\ X \end{bmatrix} \begin{matrix} 27 \\ 5 \\ 23 \end{bmatrix} \quad \begin{matrix} F \\ ? \\ P \end{bmatrix} \begin{matrix} 5 \\ 27 \\ 15 \end{bmatrix} \quad \begin{matrix} L \\ X \\ G \end{bmatrix} \begin{matrix} 11 \\ 23 \\ 6 \end{bmatrix} \quad \begin{matrix} X \\ S \\ N \end{bmatrix} \begin{matrix} 23 \\ 18 \\ 13 \end{bmatrix}$$

لذاحاصل بصورت ماتریس زیر بدست می آید:

$$C=\begin{bmatrix}17 & 3 & 5 & 22 & 22 & 2 & 27 & 5 & 11 & 23\\ 15 & 23 & 20 & 27 & 13 & 14 & 5 & 27 & 23 & 18\\ 9 & 2 & 22 & 28 & 5 & 19 & 23 & 15 & 6 & 13\end{bmatrix}$$

حال $A^{-1}C$ را که همان ماتریس رمز گشایی شده است بدست می آوریم،

$$A^{-1}C=\begin{bmatrix}16 & 24 & 22\\ 17 & 17 & 21\\ 8 & 14 & 21\end{bmatrix}\begin{bmatrix}17 & 3 & 5 & 22 & 22 & 2 & 27 & 5 & 11 & 23\\ 15 & 23 & 20 & 27 & 13 & 14 & 5 & 27 & 23 & 18\\ 9 & 2 & 22 & 28 & 5 & 19 & 23 & 15 & 6 & 13\end{bmatrix}$$

$$=\begin{bmatrix}830 & 644 & 1044 & 1616 & 774 & 786 & 1058 & 1058 & 860 & 1086\\ 733 & 484 & 887 & 1421 & 700 & 671 & 1027 & 859 & 704 & 970\\ 535 & 388 & 782 & 1142 & 463 & 611 & 769 & 733 & 536 & 709\end{bmatrix}$$

$$=\begin{bmatrix}18 & 6 & 0 & 21 & 20 & 3 & 14 & 14 & 19 & 13\\ 8 & 20 & 17 & 0 & 4 & 4 & 12 & 18 & 8 & 13\\ 13 & 11 & 28 & 11 & 28 & 2 & 15 & 8 & 14 & 13\end{bmatrix}\pmod{29}$$

و نهایتاً با استفاده از جدول(۳) دیکُد می کنیم،

$$\begin{array}{cccccccccc}S & G & A & V & U & D & O & O & T & N\\ I & U & R & A & E & E & M & S & I & N\\ N & L & \neg & L & \neg & C & P & I & O & N\\ \begin{bmatrix}18\\8\\13\end{bmatrix} & \begin{bmatrix}6\\20\\11\end{bmatrix} & \begin{bmatrix}0\\17\\28\end{bmatrix} & \begin{bmatrix}21\\0\\11\end{bmatrix} & \begin{bmatrix}20\\4\\28\end{bmatrix} & \begin{bmatrix}3\\4\\2\end{bmatrix} & \begin{bmatrix}14\\12\\15\end{bmatrix} & \begin{bmatrix}14\\18\\8\end{bmatrix} & \begin{bmatrix}19\\8\\14\end{bmatrix} & \begin{bmatrix}13\\13\\13\end{bmatrix}\end{array}$$

SINGULAR VALUE DECOMPOSITION

لذا با داشتن ماتریس کلیدی و معکوس آن به راحتی می توان عبارت های متنی را کُد، رمزی و سپس رمزگشایی و دیکُد کرد،

پروژه

۱- عبارت LINEAR ALGEBRA IS FUN را با استفاده از ماتریس کلیدی A در mod29 رمز نمایید و پیام رمز شده را به دست آورید.

$$A=\begin{bmatrix}4 & 9 & 15\\ 15 & 17 & 6\\ 24 & 0 & 17\end{bmatrix}$$

۲- ماتریس کلیدی زیر را در نظر بگیرید،

$$A=\begin{bmatrix}11 & 20 & 20\\ 2 & 1 & 24\\ 9 & 3 & 3\end{bmatrix}$$

عبارت رمز شده زیر را با استفاده از ماتریس کلیدی A در mod26 رمزگشایی و دیکد کنید.

CQUIWEHMWESTAHVPDIKUJIVPIAI

۳- **با استفاده از نرم افزار MATLAB برنامه ای بنویسید که**

الف) با دریافت عبارت متنی اصلی و ماتریس کلیدی 3x3 عبارت رمز شده حاصل در mod29 را چاپ نماید.

ب) با دریافت متن رمز شده و ماتریس کلیدی 3x3 عبارت اصلی را درmod29 بازسازی کرده و نمایش دهد.