## ۱ـ کد و رمزی کردن پیام های متنی

یکی از ساده ترین روش ها برای کد کردن پیام، جایگزین کردن هر حرف با حرف دیگر با استفاده از جدولی بصورت جدول (۱) است. این روش در بسیاری از جدول ها و معماهای موجود در مجلات مورد استفاده قرار می گیرد. در این روش فاصله بین کلمات و علامت های نگارشی در نظر گرفته نشده است.
(جدول ۱)
بطور مثال، عبارت VECTOR SPACE با این روش بصورت JGWFNSEMYWG کد می شود. برای دیکد کردن این روش از جدولی بصورت جدول (۲) استفاده می نماییم.
(جدول ۲)
بطور مثال، عبارت کد شده XPLGYSYXDGCSY با استفاده از جدول (۲) بصورت LINEAR ALGEBRA دیکد می شود. یکی از اشکالات 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 کدگذاری مربوطه را بدست آورد.

یکی دیگر از روش های کد گذاری، که در مبحث جبرخطی مطرح می گردد، استفاده از اعداد در کد کردن 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 کدگذاری استفاده می شود،
(جدول ۳)
پیام متنی SINGULAR VALUE DECOMPOSITION با استفاده از این روش با تفکیک به بردارهای سه تایی بصورت زیر کد می شود.

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

لازم به ذکر است در انتهای پیام جهت تکمیل بردار نهایی می توان حرف آخر را به تعداد مورد نیاز تکرار نمود. در مورد این مثال حرف $N$ در انتهای عبارت دو بار تکرار شده است. در نهایت 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 را با استفاده از جدول (۳) بصورت اعداد کد نماییم. حال برای رمزی کردن این پیام از یک ماتریس کلیدی معکوس پذیر $3 \times 3$ استفاده می نماییم.

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

با ضرب ماتریس کلیدی A در ماتریس P پیام رمز شده بدست می آید،

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

برای بیان این ماتریس بصورت عبارت متنی رمز شده باید درایه های ماتریس را به اعدادی در محدوده ۰ تا ۲۸ تبدیل نماییم. برای این منظور از محاسبات ماجولار یا پیمانه ای (modular arithmetic) استفاده می نماییم. در این روش هر یک از اعداد را با باقیمانده تقسیم آن عدد بر ۲۹ جایگزین می نماییم.

بطور مثال،

$$\begin{aligned} 394 = 29 \times 13 + 17 &\implies 394 \equiv 17(\mod 29) \\ 653 = 29 \times 22 + 15 &\implies 653 \equiv 15(\mod 29) \\ 415 = 29 \times 14 + 9 &\implies 415 \equiv 9(\mod 29) \\ &\vdots \end{aligned}$$

به این ترتیب ماتریس رمز شده در $\mod 29$ 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 آن 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 $G$ و $F$ و ? رمز شده است.

## ۲ـ رمزگشایی و دیکد کردن پیام های رمز شده

برای رمزگشایی عبارت های رمز شده و بازیابی پیام اصلی، از معکوس ماتریس کلیدی در $\mod 29$ استفاده می شود. برای محاسبه معکوس اعداد در $\mod 29$ بصورت زیر عمل می کنیم،

$$\begin{aligned} 2 \times 15 = 30 \equiv 1(\mod 29) &\implies \frac{1}{2} \equiv 15(\mod 29) \\ 3 \times 10 = 30 \equiv 1(\mod 29) &\implies \frac{1}{3} \equiv 10(\mod 29) \\ 4 \times 22 = 88 \equiv 1(\mod 29) &\implies \frac{1}{4} \equiv 22(\mod 29) \\ &\vdots \end{aligned}$$

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

$$A = \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \quad \rightarrow \quad A^{-1} = \frac{1}{-1635} \begin{bmatrix} 85 & -90 & -10 \\ -187 & -129 & 349 \\ -1 & 78 & -173 \end{bmatrix}$$

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

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

$$A^{-1} = \begin{bmatrix} -680 & 720 & 80 \\ 1496 & 1032 & -2792 \\ 8 & -624 & 1384 \end{bmatrix} = \begin{bmatrix} 16 & 24 & 22 \\ 17 & 17 & 21 \\ 8 & 14 & 21 \end{bmatrix}$$

می توان بررسی کرد که $A^{-1}$ بدست آمده معکوس ماتریس کلیدی $A$ در $29 \bmod$ است،

$$A^{-1}A = \begin{bmatrix} 16 & 24 & 22 \\ 17 & 17 & 21 \\ 8 & 14 & 21 \end{bmatrix} \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} = \begin{bmatrix} 726 & 646 & 1102 \\ 580 & 407 & 986 \\ 493 & 290 & 755 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \pmod{29}$$

حال از ماتریس $A^{-1}$ می توان 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،

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

لذا حاصل 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،

$$\begin{aligned} A^{-1}C &= \begin{bmatrix} 16 & 24 & 22 \\ 17 & 17 & 21 \\ 8 & 14 & 21 \end{bmatrix} \begin{bmatrix} 17 & 3 & 5 & 22 & 22 & 2 & 27 & 5 & 11 & 23 \\ 15 & 23 & 20 & 27 & 13 & 14 & 5 & 27 & 23 & 18 \\ 9 & 2 & 22 & 28 & 5 & 19 & 23 & 15 & 6 & 13 \end{bmatrix} \\ &= \begin{bmatrix} 830 & 644 & 1044 & 1616 & 774 & 786 & 1058 & 1058 & 860 & 1086 \\ 733 & 484 & 887 & 1421 & 700 & 671 & 1027 & 859 & 704 & 970 \\ 535 & 388 & 782 & 1142 & 463 & 611 & 769 & 733 & 536 & 709 \end{bmatrix} \\ &= \begin{bmatrix} 18 & 6 & 0 & 21 & 20 & 3 & 14 & 14 & 19 & 13 \\ 8 & 20 & 17 & 0 & 4 & 4 & 12 & 18 & 8 & 13 \\ 13 & 11 & 28 & 11 & 28 & 2 & 15 & 8 & 14 & 13 \end{bmatrix} \pmod{29} \end{aligned}$$

و نهایتا با استفاده از جدول (۳) دیکد می کنیم،

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

SINGULAR VALUE DECOMPOSITION

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

### ۳ـ پروژه

۱ ـ معکوس اعداد ۱ تا ۲۸ را در $29 \bmod$ و اعداد ۱ تا ۲۵ را در $26 \bmod$ بدست آورید و آن ها را در دو جدول جداگانه نمایش دهید. آیا تمام اعداد در $29 \bmod$ و در $26 \bmod$ معکوس پذیر هستند؟چه نتیجه ای می گیرید؟

۲ـ یک ماتریس تحت چه شرایطی در $\mod 29$ و در $\mod 26$ معکوس پذیر است. معکوس ماتریس $A$ را یکبار در $\mod 29$ و یکبار در $\mod 26$ بدست آورید.

$$A = \begin{bmatrix} 21 & 24 & 2 \\ 0 & 1 & 3 \\ 21 & 19 & 17 \end{bmatrix}$$

۳ـ عبارت LINEAR ALGEBRA IS FUN را با استفاده از ماتریس کلیدی $A$ در $\mod 29$ رمز نمایید و پیام رمز شده را بدست آورید.

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

۴ـ 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 $\mod 26$ رمز گشایی و دیکد کنید.

CQUIWEHMWESTAHVPDIKUJIVPIAI

۵ـ اگر عبارت HILLCIPHER توسط ماتریس کلیدی $A_{2\times 2}$ در $\mod 29$ بصورت $JK.M\neg TWIBO$ رمز شده باشد، ماتریس کلیدی $A_{2\times 2}$ را برای این رمزنگاری بدست آورید.

۶ـ با استفاده از نرم افزار MATLAB برنامه ای بنویسید که،
الف) با دریافت عبارت متنی اصلی و ماتریس کلیدی $3 \times 3$، عبارت رمز شده حاصل در $\mod 29$ را چاپ نماید.
ب) با دریافت متن رمز شده و ماتریس کلیدی $3 \times 3$ عبارت اصلی را در $\mod 29$ بازسازی کرده و نمایش دهد.

جهت مطالعه بیشتر می توانید از مراجع زیر استفاده نمایید.
http://practicalcryptography.com/ciphers/hill-cipher/
http://en.wikipedia.org/wiki/Hill-cipher