Computational Cryptography

التشفير الحسابي

بتطبيق الرياضيات والحاسب الالكتروني في تقنيات التشفير، فانه من الممكن التوسع الى ابعد من تقنيات التشفير القياسية التي تمت مناقشتها الى حد الآن. إن الحسابات التي يمكن تطبيقها على التقنيات المشروحة سابقا تتضمن العمليات الحسابية كالجمع والطرح والضرب والقسمة. بالاضافة الى ذلك، فان العمليات الجبرية وعمليات المصفوفة يمكن ان تضم الى تقنيات التشفير التقليدية. ان كلاً من هذه العمليات الحسابية سيتم مناقشتها في هذا البند.

Arithmetic Operations

العمليات الحسابية

إن رسالة النص الصريح يمكن تشفيرها بسهولة باستخدام العمليات الحسابية بصفتها مفتاحاً. ولاجل التوضيح، سنستخدم الرسالة الاتية :-

CHANGE KEYS TODAY

فاذا ابدل كل من هذه الحروف بقيمة آسكي المكافئة، فان النص الصريح سيصبح شفرة تعويضية بصورة متوالية من اعداد ذوات رقمين وكالاتي :-

النص الصريح	قيمة آسكي					
CHANGE	67	72	65	78	71	69
KEYS	75	69	89	83		
TODAY	84	79	68	65	89	

فاذا ميزت هذه الاعداد بصفتها قيم آسكي فان هذا سيقدم لنا الرسالة المشفورة، وبتطبيق واحد او اكثر من العمليات الحسابية عليها نتمكن من تمويه هذه الاعداد. وبطرح العدد 50 من كل قيمة من قيم اسكي نحصل على :

النص الصريح	50 - قيمة اسكي					
CHANGE	17	22	15	28	21	29
KEYS	25	19	39	33		
TODAY	34	29	18	15	39	

واذا ضربنا بالقيمة 20، فاننا سنحصل على متوالية من القيم وكالاتي:

النص الصريح	20 × (قيمة اسكي)					
CHANGE	13.4	14.4	13.0	15.6	14.2	13.8
KEYS	15.0	13.8	17.8	16.6		
TODAY	16.8	15.8	13.6	13.0	17.8	

ماشرحناه هنا يوضح بأنه يمكن تشفير النص الصريح باستخدام واحد من المفاتيح الاربعة المعتمِدة على قيم اسكي. وهذه المفاتيح الاربعة هي:

1. (قيمة الـ ASCII) + قيمة ثابتة ← حرف مشفور
2. (قيمة الـ ASCII) − قيمة ثابتة ← حرف مشفور
3. (قيمة الـ ASCII) × قيمة ثابتة ← حرف مشفور
4. (قيمة الـ ASCII) ÷ قيمة ثابتة ← حرف مشفور

العمليات الجبرية Algebraic Operations

سنتناول هنا طرائق وعمليات انتاج النصوص المشفورة من النص الواضح والتي تتجاوز العمليات الحسابية البسيطة كالجمع والطرح والضرب والقسمة. فسابقا كانت التعابير الحسابية مثل الاتي:

$$B(I) + C$$

حيث ان B (I) هو مكافيء ASCII العددي، والـ C تمثل قيمة ثابتة. وهذا التعبير يحتوي على عملية اساسية وحيدة ـ هي عملية الجمع. ان استخدام اكثر من عملية وحيدة يجهزنا بالتعابير الجبرية التي تنتج شفرات تعويضية محسنة واكثر امنية.

المعادلات الخطية Linear Equations

إن التعبير الجبري الشائع هو معادلة الخط المستقيم:

$$y = a + bx$$

حيث ان الـ a هو قيمة y عندما تكون x تساوي صفرا، او قطع الـ y و b هو الميل، و x هي قيمة والـ y هو الناتج. إن أية قيمة تعطى لـ x والتي تؤدي الى y، تعطينا نقطة (x، y) على المخطط البياني.

والان، كيف يمكن لمثل هذا التعبير الجبري $y = a + bx$ ان يستخدم في التشفير؟ عموماً، نحن نرغب بتمويه نتيجة النص المشفور بحيث يكون من الصعب للافراد غير المخولين ان يفكوا هذا النص المشفور. ومع ذلك فنحن نريد عملية «بسيطة» للتشفير بالاضافة الى عملية بسيطة لفك الشفرة. إن التعبير الجبري، مثل المثال السابق، يمكن ان يساعدنا للوصول الى طريقة بسيطة. ولتوضيح هذه الطريقة، فان التعبير الجبري $y = a + bx$ يحتاج الى توفير هذين الثابتين.

ان هذين الثابتين هما بالحقيقة، المفتاح المطلوب في عمليتي التشفير وفك الشفرة. فاذا قررنا بان المفتاح سيكون 2، (1 / 2)، فعندئذ:

$$y = 2 + 1/2\ x$$

والـ x سيكون مكافىء ASCII العددي بعد تغيير الرسالة من هيأة السلسلة الى قيمة ASCII.
ولتوضيح هذه الطريقة، دعنا نقول إن الرسالة المطلوب تشفيرها هي:

CHANGE KEYS TODAY

إن هذا النص الصريح، عندما يتحول الى قيم آسكي ذوات مرتبتين عشريتين، يصبح كالاتي:

النص الصريح	قيمة اسكي					
CHANGE	67	72	65	78	71	69
KEYS	75	69	89	83		
TODAY	84	79	68	65	89	

إن قيم اسكي سوف تتحول الى مجموعة جديدة من القيم المشفورة بوساطة العملية الاتية:

قيمة جديدة = (قيمة ASCII) 2/ 1 + 2

وللمثال، فان الحرف C يساوي 67 في الآسكي، لذا فان العملية تعطي القيم الجديدة الاتية:

$$2 + 1 / 2 (67) = 2 + 33.5 = 35.5$$

ستتمكن بعد ذلك من ايجاد قيمة جديدة لكل حرف من حروف النص الصريح، وهذه القيم الجديدة يمكن استخدامها باعتبارها النص المشفور. إن النص المشفور الكامل للرسالة المذكورة اعلاه يكون كالاتي:

النص الصريح	النص المشفور					
CHANGE	35.5	38	34.5	41	37.5	36.5
KEYS	39.5	36.5	46.5	43.5		
TODAY	44	41.5	36	34.5	46.5	

لو كان الشخص غير المخول يعرف التعبير الجبري المستخدم للحصول على هذا النص المشفور، فان تخميناً موفقاً سيكون كافياً لحل شفرتها. وفي الفصل القادم سنرى التقنيات التي يمكن استخدامها لتحليل وفك مثل هذه الرسائل بدون معرفة المفتاح.

إن نصنا المشفور يملك كلاً من الاعداد الكاملة والقيم الكسرية. إن القيمة مثل 35.5 تدل على ان بعض عمليات التشفير الجبري قد استخدمت.

ولاخفاء استخدامنا للتعبير الجبري في عملية التشفير، فان المفتاح يمكن ان يستخدم والذي ينتج عن اعداد صحيحة فقط. ومع مثل هذا التعبير y = a + bx، فهناك عدد غير محدود من الاحتمالات بالنسبة للمفتاح a و b لانتاج عدد كامل من القيم المشفورة. فكل مانحتاجه هو ان كلاً من a و b يكونان اعداداً صحيحة. ان كلاً من a و b او كليهما يمكن ان يكونا اعداداً صحيحةً سالبة فاذا استخدم المفتاح 15 - و 2 مع النص الصريح فان النواتج ستكون كالاتي:

لفك شفرة الرسالة بالاعتماد على قيم الاعداد المشتقة من العمليات الجبرية سنحتاج الى عكس العملية. ولمثالنا المذكور، فعند الرجوع من النص المشفور الى النص الصريح نتبع هذه العملية:

قيم النص المشفور ← معادلة فك الشفرة ← قيم اسكي الاصلية ← التحويل الى النص الصريح

وللحصول على معادلة فك الشفرة يجب ان نحل معادلة التشفير جبرياً. ان هذه المعادلة كانت هي التعبير الاتي:

$$y = a + bx$$

حيث ان x قد استخدم لانتاج y

والان نبدأ بالقيمة y ونجرب ايجاد قيمة x. وذلك بنقل الحدود، فسيكون عندنا

$$bx = y - a$$

عندئذ سيكون

$$x = (y - a) / b$$

إن الناتج النهائي هو النص الواضح مع فجوات موضوعة في الداخل كالاتي:

النص المشفور: 119 129 115 141 127 (123) 135 (123)
163 151 153 143 121 115 163

النص الصريح: CHANGE KEYS TODAY

وبما ان الاعادة للنص المشفور يمكن ان توفر لمحلل الشفرة الدليل لكسر الشفرة، لذا فأنه من المفيد ان نموه النتائج بحيث ان كل حروف الـ E من النص الواضح لن تُشفر مثل الرقم 123. وهذه الحالة كانت عند استخدام المفتاح $a = -15$، و $b = 2$.

عندما يكون الحاسب قادراً على العمل مع حروف هجائية او متسلسلة في جدول او مصفوفة، فان عمليات التشفير وفك الشفرة يمكن ان تطور باستخدام فكرة جبر المصفوفة.

في المصفوفة، يتغير النص الصريح الى قيم عددية من الآسكي. ومع مثل هذه القيم العددية، يمكن انجاز مختلف التحويلات على المصفوفة وللمثال على ذلك، يمكن ان تضرب المصفوفة بقيمة ثابتة لتكوين مصفوفة جديدة، وينتج عن ذلك مجموعة من النصوص المشفورة في طريقة مشابهة الى التحويلات الجبرية.

ان احدى عمليات المصفوفة الاخرى التي يمكن استخدامها للتشفير هي عملية ابدال المصفوفة. فهنا يتحول النص الصريح الى قيم تعويضية. وباستخدام عملية ابدال المصفوفة، سيظهر نص مشفور جديد. وهذا النوع من النص المشفور يدعى نصاً مشفوراً مركباً. وهذا يعني انه يعتمد على كل من عمليتي التعويض والابدال.

واضافة الى ذلك، فهناك عمليات مصفوفة اخرى يمكن ان تبرمج لانجاز عملية تشفير النص الصريح. إن النص المشفور يمكن ان يطور باستخدام عملية عكس المصفوفة الى مصفوفة بقيم آسكي.

إن عمليات المصفوفة الثلاث المذكورة هنا تستخدم كلمة النص الصريح DATA. وكل توضيح يتبع تحويل المصفوفة الاتية:

$$\begin{pmatrix} D & A \\ T & A \end{pmatrix}$$

الى قيم آسكي:-

$$\begin{pmatrix} 68 & 65 \\ 84 & 65 \end{pmatrix}$$

Encryption by Matrix Multiplication التشفير بالضرب المصفوفي

إذا كانت مصفوفة قيم آسكي يرمز لها بالرمز V، لذا عند ضربها بقيمة ثابتة او بالمفتاح K، فان الناتج هو مصفوفة نص مشفور جديدة، C، اي ان:

$$C = (K) \times V$$

فاذا كان المفتاح هو $k = 2$، فالناتج هو:

$$C = 2 \times \begin{pmatrix} 68 & 65 \\ 84 & 65 \end{pmatrix} = \begin{pmatrix} 136 & 130 \\ 168 & 130 \end{pmatrix}$$

ان النص المشفور النهائي، اذا اخذ من الـ C بصورة افقية، يصبح متوالية من الاعداد هي:

136 130 168 130

تمثل كلمة النص الصريح DATA

التشفير بالابدال المصفوفي Encryption by Matrix Transposition

ان إبدال المصفوفة الجبري هو:

$$C = V^T$$

حيث ان الـ V^T يشير الى ان الصفوف والاعمدة للمصفوفة V قد تبادلت. هذا يعني بأن مصفوفة قيم اسكي.

$$V = \begin{pmatrix} 68 & 65 \\ 84 & 65 \end{pmatrix}$$

تصبح مصفوفة النص المشفور

$$C = V^T = \begin{pmatrix} 68 & 84 \\ 65 & 65 \end{pmatrix}$$

واذا كانت قيم الـ C تأخذ افقياً، فأن النتيجة هي نص مشفور مركب (التعويض والابدال).

68 84 65 65

يمثل كلمة النص الصريح DATA

التشفير بالعكس المصفوفي Encryption by Matrix Inversion

إن عملية عكس المصفوفة هي عملية مناظرة لايجاد معكوس القيمة. لذا، فاذا كان $x = 4$، فان المعكوس x^{-1} يساوي $1 / x$ أو $1 / 4$. ولانتاج نص مشفور باستخدام معكوس المصفوفة لقيم اسكي، فان معادلة المعكوس هي:

$$C = V^{-1}$$

والتي تشير الى ان المصفوفة V معكوسة. إن هذا العكس هو:

$$C = \begin{pmatrix} -.0625 & .0625 \\ .0808 & -.0654 \end{pmatrix}$$

فاذا اخذت هذه القيم بصورة افقية، فان هذا سيولد نصاً مشفوراً هو:

-0625 .0625 .0808 -0654

لكلمة النص الصريح DATA. إن عكس المصفوفة يمكن ان يجري فقط على المصفوفات المربعة. ومع ذلك فانه ليست جميع المصفوفات المربعة تملك معكوساً.

الحرف	القيمة	الحرف	القيمة	الحرف	القيمة
	32	6	54	K	75
!	33	7	55	L	76
"	34	8	56	M	77
#	35	9	57	N	78
$	36	:	58	O	79
%	37	;	59	P	80
&	38	<	60	Q	81
'	39	=	61	R	82
(	40	>	62	S	83
)	41	?	63	T	84
*	42	@	64	U	85
+	43	A	65	V	86
,	44	B	66	W	87
-	45	C	67	X	88
.	46	D	68	Y	89
/	47	E	69	Z	90
0	48	F	70	[	91
1	49	G	71	\	92
2	50	H	72	]	93
3	51	I	73	^	94
4	52	J	74	_	95
5	53				

جروف(ASCII)