جامعة المنارة
كلية الهندسة
قسم المعلوماتية

Information System Security
أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا

الجلسة السادسة

المسألة الأولى

بفرض لدينا $X = (X_0,X_1,X_2,...,X_{n-1})$ Data حيث X_i هي عبارة عن بايت ، إذا فرضنا تابع بعثرة hash يعرف كالآتي:

$$h(X) = X_0+X_1+X_2+...+X_{n-1}$$

هل هو آمن ؟ وضح إجابتك

الحل:

كلا ليس آمن . مثال: بفرض X0=10101010 , X1=00001111

فتكون: X = (X0,X1) = (10101010,00001111)

$$h(X) = 10101010+00001111=10111001$$

فتكون: Y = (X1,X0) = (00001111, 10101010)

$$h(Y) = 00001111+10101010=10111001$$

أنه غير مقاوم للتصادمات حيث نلاحظ أن $Y \neq X$ لكن h(X)=h(Y) فهو تابع غير آمن.

المسألة الثانية

بفرض لدينا تابع البعثرة الآتي : $h(X) = \sum_i^n a_i \ mod\ 10$

حيث a_i المقابل العددي للمحرف بالعشري من جدول الأسكي

١. احسب خرج هذا التابع من أجل الدخلين الآتيين وماذا تلاحظ؟ وماذا تسمى هذه الخاصية؟

- X1=hello
- X2=Hello

٢. احسب خرج تابع البعثرة السابق من أجل X=world .ماذا تلاحظ؟

٣. برأيك هل يمكن أن يستخدم هذا التابع في التطبيقات الأمنية؟ علل إجابتك.

حل المسألة

الطلب الأول: من جدول الأسكي نجد :

المحرف	بالثنائي	بالعشري
h	1100101	101
e	1101000	104
l	1101100	108
o	1101111	111
H	1001000	72

$$h(hello) = \sum_{i=1}^{5} a_i \ mod\ 10$$
$$= (101 + 104 + 108 + 108 + 111) mod 10$$
$$= 532 mod 10 = 2$$

$$h(Hello) = \sum_{i=1}^{5} a_i \ mod\ 10$$
$$= (72 + 104 + 108 + 108 + 111) mod 10$$
$$= 503 mod 10 = 3$$

نلاحظ أن تغير بسيط في الدخل أعطى خرجاً مختلفاً تماماً . تسمى خاصية الانهيار الثلجي

المحرف	بالثنائي	بالعشري
w	1110111	119
r	1110010	114
l	1101100	108
o	1101111	111
d	1100100	100

الطلب الثاني:

$$h(world) = \sum_{i=1}^{5} a_i \ mod\ 10$$
$$= (119 + 111 + 114 + 108 + 100) mod 10$$
$$= 552 mod 10 = 2$$

نلاحظ أن هذا التابع غير مقاوم للتصادم لأن: **h(hello)= h(world)=2**

الطلب الثالث:

3. لا ينصح باستخدامه في التطبيقات الأمنية لأنه غير أمن لأنه غير مقاوم للتصادمات

	000	001	010	011	100	101	110	111
0000	NULL	DLE		0	@	P	`	p
0001	SOH	DC1	!	1	A	Q	a	q
0010	STX	DC2	"	2	B	R	b	r
0011	ETX	DC3	#	3	C	S	c	s
0100	EDT	DC4	$	4	D	T	d	t
0101	ENQ	NAK	%	5	E	U	e	u
0110	ACK	SYN	&	6	F	V	f	v
0111	BEL	ETB	'	7	G	W	g	w
1000	BS	CAN	(	8	H	X	h	x
1001	HT	EM	)	9	I	Y	i	y
1010	LF	SUB	*	:	J	Z	j	z
1011	VT	ESC	+	;	K	[	k	{
1100	FF	FS	,	<	L	\	l	|
1101	CR	GS	-	=	M	]	m	}
1110	SO	RS	.	>	N	^	n	~
1111	SI	US	/	?	O	_	o	DEL

المحرف	بالثنائي	بالعشري
w	1110111	119
r	1110010	114
l	1101100	108
o	1101111	111
d	1100100	100

جامعة المنارة
MANARA UNIVERSITY

المسألة الثالثة

بفرض لدينا تابع البعثرة الآتي : $h(X)=\sum_i^n a_i \ mod\ 26$

حيث a_i المقابل العددي للمحرف بالعشري من جدول الأسكي

١. احسب خرج هذا التابع من أجل الدخلين الآتيين وماذا تلاحظ؟ وماذا تسمى هذه الخاصية؟

- X1=CAT
- X2=DOG

٢. هل يمكن أن تجد حالة تصادم؟ وضح ذلك

حل المسألة

الطلب الأول: من جدول الأسكي نجد :

المحرف	بالثنائي	بالعشري
C	1000011	67
A	1000001	65
T	1010100	84

$$h(CAT) = \sum_{i=1}^{3} a_i \; mod 26 = (67 + 65 + 84) mod 26$$
$$= 216 mod 26 = 8$$

المحرف	بالثنائي	بالعشري
D	1000100	68
O	1001111	79
G	1000111	71

$$h(DOG) = \sum_{i}^{3} a_i \; mod \; 26 = (68 + 79 + 71) mod 26$$
$$= 218 \; mod 26 = 10$$

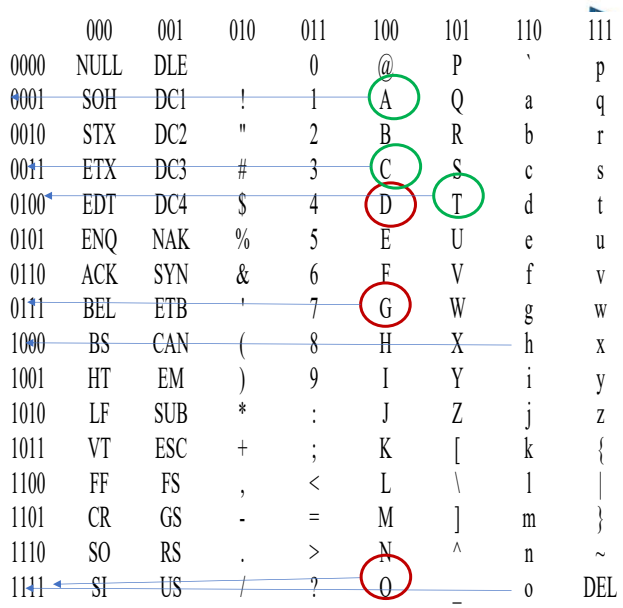
حل المسألة

الطلب االثاني : نعم يمكن إيجاد تصادم كالآتي

المحرف	بالثنائي	بالعشري
C	1000011	67
A	1000001	65
T	1010100	84

$$CAT \neq ACT \, , \, h(ACT) = h(CAT)$$

$$h(ACT) = \sum_{i=1}^{3} a_i \; mod 26 = (65 + 67 + 84) mod 26$$
$$= 216 mod 26 = 8 = \; h(CAT)$$



	000	001	010	011	100	101	110	111
0000	NULL	DLE		0	@	P	`	p
0001	SOH	DC1	!	1	A	Q	a	q
0010	STX	DC2	"	2	B	R	b	r
0011	ETX	DC3	#	3	C	S	c	s
0100	EDT	DC4	$	4	D	T	d	t
0101	ENQ	NAK	%	5	E	U	e	u
0110	ACK	SYN	&	6	F	V	f	v
0111	BEL	ETB	'	7	G	W	g	w
1000	BS	CAN	(	8	H	X	h	x
1001	HT	EM	)	9	I	Y	i	y
1010	LF	SUB	*	:	J	Z	j	z
1011	VT	ESC	+	;	K	[	k	{
1100	FF	FS	,	<	L	\	l	|
1101	CR	GS	-	=	M	]	m	}
1110	SO	RS	.	>	N	^	n	~
1111	SI	US	/	?	O	_	o	DEL

المحرف	بالثنائي	بالعشري
C	1000011	67
A	1000001	65
T	1010100	84

المحرف	بالثنائي	بالعشري
D	1000100	68
O	1001111	79
G	1000111	71

جامعة المنارة
MANARA UNIVERSITY

المسألة الرابعة

إذا كان لديك تابع بعثرة بخرج 80 بت والمطلوب:

١. ما عدد المحاولات لإيجاد تصادم باحتمال 25% ؟

٢. إذا كان جهازك يحسب (H/SEC) 100 . كم الوقت اللازم لإيجاد التصادم؟

حل المسألة

١. عدد المحاولات لإيجاد تصادم باحتمال 25%

$$k \approx \sqrt{2N\ ln\left(\frac{1}{1-p}\right)}$$

عدد القيم الممكنة : $N = 2^n = 2^{80} = 1.21 \times 10^{24}$

نعوض في علاقة عدد المحاولات لإيجاد تصادم

$$k \approx \sqrt{2 \times 1.21 \times\times 10^{24} ln\left(\frac{1}{1-0.25}\right)}$$

$k \approx 2.64 \times 10^{12}$ محاولة

٢. الزمن اللازم لإيجاد التصادم:

$$T(sec) = \frac{k}{V} = \frac{2.64 \times 10^{12}}{10^8} = 26400\ \text{sec} \approx 7.3\ hours$$

المسألة الخامسة

أكمل الجدول الآتي:

طول خرج تابع البعثرة(بت)	القيم الممكنة	عدد المحاولات للتصادم بـ 50%	عدد المحاولات للتصادم بـ 90%
64			
128			

حل المسألة

بالاعتماد على العلاقات الاتية

$k \approx 2.146\sqrt{N}\ ; P = 0.9$ $\quad k \approx 1.1774\sqrt{N}\ ; P = 0.5$ $\quad N = 2^n$: عدد القيم الممكنة

طول خرج تابع البعثرة(بت)	القيم الممكنة	عدد المحاولات للتصادم بـ 50%	عدد المحاولات للتصادم بـ 90%
64	1.84×10^{19}	5.06×10^{9}	9.22×10^{9}
128	3.40×10^{38}	2.17×10^{19}	3.96×10^{19}

نهاية الجلسة