บรรณานุกรม

Cooper. James Arlin .Computer and Communications Securities : Stretegies for the 1990s. Intertext Publications / Multi Science Press.1989.

Davies. D. W. and W. L. Price. Security for Computer Networks : An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer. Jonh Wiley and sons. 1984.

Denning. Dorothy Elizabeth Robing. Cryptography and Data Security. Addison-Wesley. 1982.

Diffie. Whitfield and Martin E. Hellman. "New Directions in Cryptography". Trans. IEEE on Information Theory. IT-22. 6. (November 1976):644-654.

Diffie. Whitfield and Martin E. Hellman. "Exhaustive Cryptanalysis of the NBS Data Encryption Standard". Computer. (June 1977): 74-84.

Gordon. J.A. and Retkin. H. "Are big S-boxes best?" Cryptography (Proceedings. Burg Feuerstein 1982. Ed. T. Beth). Lecture Notes in Computer Science 149. Springer Verlag. Berlin. 1983.

Hellman. Martin E., "DES will be totally insecure within ten years". IEEE Spectrum. (July 1979):32-39.

Laudon. Kenneth C. and Jane Price Laudon. Management Information Systems : A Contemporary Perspective. Macmillan Publishing Company. 1988.

Meissner. P.(Ed). "Report of the workshop on Estimation of Significant Advance in Computer Technology". National Bureau of Standards. Report NBSIR . (December 1976):76-1189.

Meyer. H. Carl and Stephen M. Matyas. Cryptography : A New Dimension in Computer Security. John Wiley and sons. 1982.

National Bureau of Standards. "Data Encryption Standard", Federal Information Processing Standards Publication 46.(January 1977).

Patterson. Wayne. Mathematical Cryptology for Computer Scientists and Mathematicians. Rand and Littlefield. 1987.

Seberry. Jennifer and Josef Pieprzyk. Cryptography : An Introduction to Computer Security. Prentice Hall. 1989.

Shannon. C. E.."Communication Theory of Secrecy System". The Bell System Technical Journal. vol. 28. no.4. 1949.

Sugarman. Robert. "On Foiling Computer Crime".IEEE Spectrum. 16. 7. 32. July. 1979.

ภาคผนวก

ผลการทดสอบการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อข้อมูลเนื้อแท้
เปลี่ยนไป 1 บิต ของอัลกอริทึมเดสและอัลกอริทึมไอเดสกรณีต่าง ๆ

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 6 6 6 6 6 6 6 6
ข้อมูลออก แบ่งเป็นกลุ่มละ 4 4 4 4 4 4 4 4
คีย์สำหรับเข้ารหัสลับ : 0123456789abcdef

ข้อมูลเนื้อแท้	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
4142434445464748	fa46606cfc0449cc	
5142434445464748	1ef14aaf0c1b5a5d	32
4152434445464748	a7f1ec48031d466a	35
4142534445464748	f112933f28920651	34
4142435445464748	de1d68c4f0053eb1	26
414243445546474e	988abf8eb923fced	32
41424344454e4748	652a4dc43c0fd4d0	30
4142434445465748	5db4bf3e23eee102	40
4142434445464758	537c19d989e1fe18	38
6142434445464748	bf2759106fc1ff43	33
4162434445464748	197b7c1fd81052d6	29
4142634445464748	d2ad6239df194c24	26
4142436445464748	3871a16af4175ccd	21
4142434465464748	9f825e77fe381d06	28
4142434445464768	ebdceb18faa57792	29
ค่าเฉลี่ยระยะแฮมมิ่ง		30.93

ตารางที่ 1 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อข้อมูลเนื้อแท้
มีความแตกต่างกัน 1 บิต เมื่อใช้อัลกอริทึมเดส

หมายเหตุ : ข้อมูลเนื้อแท้และข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัส ในตารางแสดงเป็นตัวเลข
อยู่ในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 5 5 5 5 5 5 5 5 8
ข้อมูลออก แบ่งเป็นกลุ่มละ 3 3 3 3 3 3 3 3 8
คีย์สำหรับเข้ารหัสลับ : 0123456789abcdef

ข้อมูลเนื้อแท้	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
4142434445464748	9d96b959e1bc384f	
5142434445464748	efa52f148e1991e2	35
4152434445464748	4d66803ac180fb1b	27
4142534445464748	f03791cefd107a9e	28
4142435445464748	35924ac287573d79	31
414243445546474e	bd40fcbe1ae2ec27	34
41424344454e4748	569283bbc837e530	34
4142434445465748	2a6de771514d3f18	36
4142434445464758	3ccb69edcd226b1b	30
6142434445464748	9195eb2d46b8fc69	23
4162434445464748	e83506ab0e74562a	40
4142634445464748	45a09cf41412036f	33
4142436445464748	79fdee9b67de7c91	31
4142434465464748	a4750f92f08d258b	31
4142434445464768	b45860c9bb27f174	33
ค่าเฉลี่ยระยะแฮมมิ่ง		31.86

ตารางที่ 2 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อข้อมูลเนื้อแท้
มีความแตกต่างกัน 1 บิต เมื่อใช้อัลกอริทึมไอเดส กรณีที่ 1

หมายเหตุ : ข้อมูลเนื้อแท้และข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัส ในตารางแสดงเป็นตัวเลข
อยู่ในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 6 6 6 6 12 12
ข้อมูลออก แบ่งเป็นกลุ่มละ 4 4 4 4 8 8
คีย์สำหรับเข้ารหัสลับ : 0123456789abcdef

ข้อมูลเนื้อแท้	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
4142434445464748	aeea42ebc1b2f976	
5142434445464748	bffcb7a5456fdcff	29
4152434445464748	1cbb83c216129f34	27
4142534445464748	9c87acb8d07d3aa8	36
4142435445464748	e972003eac4c24ff	35
414243445546474e	53a87a3deda12768	33
41424344454e4748	edc10207e90b7bab	28
4142434445465748	207e0fdda2211a02	32
4142434445464758	76efb79f2d4c884d	37
6142434445464748	afb6e7c1ce2ed8c8	28
4162434445464748	5dba6da562c7032d	37
4142634445464748	7af3aa5c5e77b412	34
4142436445464748	e1e31898418f99fe	26
4142434465464748	0d47dc966588dee7	34
4142434445464768	71af902a51f4ba2b	30
ค่าเฉลี่ยระยะแฮมมิ่ง		31.86

ตารางที่ 3 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อข้อมูลเนื้อแท้
มีความแตกต่างกัน 1 บิต เมื่อใช้อัลกอริทึมไอเดส กรณีที่ 2

หมายเหตุ : ข้อมูลเนื้อแท้และข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัส ในตารางแสดงเป็นตัวเลข
อยู่ในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 7 7 7 7 7 7 6
ข้อมูลออก แบ่งเป็นกลุ่มละ 5 5 5 5 4 4 4
คีย์สำหรับเข้ารหัสลับ : 0123456789abcdef

ข้อมูลเนื้อแท้	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
4142434445464748	e21892969e587202	
5142434445464748	0a62f674f61c8393	29
4152434445464748	e7f3a19f4afc4786	27
4142534445464748	ffea46b2010e306e	31
4142435445464748	7a0c85a5df647709	24
414243445546474e	c0f83399f43695b2	30
41424344454e4748	268bf952767b0c01	30
4142434445465748	2c03ebfe1de2ed6b	35
4142434445464758	818119544376701b	29
6142434445464748	a866e4cd5b236ccd	39
4162434445464748	3f17064a56076406	31
4142634445464748	2d01ec129160849f	35
4142436445464748	496becc39ec10230	30
4142434465464748	34fa697a4d9e7a3b	35
4142434445464768	7a00ca2c803b1e75	31
ค่าเฉลี่ยระยะแฮมมิ่ง		31.14

ตารางที่ 4 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อข้อมูลเนื้อแท้
มีความแตกต่างกัน 1 บิต เมื่อใช้อัลกอริทึมไอเดส กรณีที่ 3

หมายเหตุ : ข้อมูลเนื้อแท้และข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัส ในตารางแสดงเป็นตัวเลข
อยู่ในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 8 8 8 8 8 8
ข้อมูลออก แบ่งเป็นกลุ่มละ 6 6 6 6 4 4
คีย์สำหรับเข้ารหัสลับ : 0123456789abcdef

ข้อมูลเนื้อแท้	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
4142434445464748	32499389f539f680	
5142434445464748	516322057a67bd01	30
4152434445464748	b53e5aa8a9c3cdff	38
4142534445464748	c0edfe6cd4789722	28
4142435445464748	ac8f4084604ecef5	35
414243445546474e	11b28591365b9b56	32
41424344454e4748	a5771974944f5e51	35
4142434445465748	4424a664ce0bf9e8	35
4142434445464758	ff65ad57fac9075a	37
6142434445464748	7ca10f99bc68237a	30
4162434445464748	b2644ee1236ccb4f	34
4142634445464748	905face6c533e02d	30
4142436445464748	e04dc0d44497fd86	28
4142434465464748	3554f908db1993ad	26
4142434445464768	92d8ac59ac6aec26	29
ค่าเฉลี่ยระยะแฮมมิ่ง		31.93

ตารางที่ 5 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อข้อมูลเนื้อแท้
มีความแตกต่างกัน 1 บิต เมื่อใช้อัลกอริทึมไอเดส กรณีที่ 4

หมายเหตุ : ข้อมูลเนื้อแท้และข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัส ในตารางแสดงเป็นตัวเลข
อยู่ในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 5 6 10 8 9 10
ข้อมูลออก แบ่งเป็นกลุ่มละ 3 4 7 5 6 7
คีย์สำหรับเข้ารหัสลับ : 0123456789abcdef

ข้อมูลเนื้อแท้	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
4142434445464748	07cdae1ba8d16ee2	
5142434445464748	ab05e62a35acf285	32
4152434445464748	25e1d2ddbdd77080	26
4142534445464748	df57796428c13242	29
4142435445464748	434b30e2856ea7a9	35
414243445546474e	64a491baf872a924	32
41424344454e4748	387ca245aad2136f	30
4142434445465748	6d4da6f8d1871886	28
4142434445464758	4c3ac75491cabe62	32
6142434445464748	7051014af393bd33	35
4162434445464748	7fdd5b6ae8088742	28
4142634445464748	982209db69a7d443	36
4142436445464748	f524b0a2df4d20b5	38
4142434465464748	5a06a3f88f5f753a	34
4142434445464768	685734c845d2104a	36
ค่าเฉลี่ยระยะแฮมมิ่ง		32.21

ตารางที่ 6 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อข้อมูลเนื้อแท้
มีความแตกต่างกัน 1 บิต เมื่อใช้อัลกอริทึมไอเดส กรณีที่ 5

หมายเหตุ : ข้อมูลเนื้อแท้และข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัส ในตารางแสดงเป็นตัวเลข
อยู่ในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 7 10 12 8 11
ข้อมูลออก แบ่งเป็นกลุ่มละ 5 6 8 6 7
คีย์สำหรับเข้ารหัสลับ : 0123456789abcdef

ข้อมูลเนื้อแท้	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
4142434445464748	9faca37cf9418a21	
5142434445464748	ff0feca0e340a16c	28
4152434445464748	17c51987d5600f47	30
4142534445464748	d37b7c63cb9eead5	38
4142435445464748	4c5867876f818eed	31
414243445546474e	bdee4020aae1ac7c	27
41424344454e4748	e867df072668f723	39
4142434445465748	4f0e15cfeacb0a83	26
4142434445464758	98287359adf14788	26
6142434445464748	859373ab05e6a953	36
4162434445464748	8eb49655aa07f334	26
4142634445464748	93511deee4477103	33
4142436445464748	510905c2b56e31bb	37
4142434465464748	28647fc7582f483c	35
4142434445464768	b41f27ae8ff24106	34
ค่าเฉลี่ยระยะแฮมมิ่ง		31.86

ตารางที่ 7 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อข้อมูลเนื้อแท้ มีความแตกต่างกัน 1 บิต เมื่อใช้อัลกอริทึมไอเดส กรณีที่ 6

หมายเหตุ : ข้อมูลเนื้อแท้และข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัส ในตารางแสดงเป็นตัวเลขอยู่ในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 12 8 6 10 12
ข้อมูลออก แบ่งเป็นกลุ่มละ 8 5 4 7 8
คีย์สำหรับเข้ารหัสลับ : 0123456789abcdef

ข้อมูลเนื้อแท้	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
4142434445464748	2fca89c940db84eb	
5142434445464748	8e09200106ccf6dd	29
4152434445464748	a4906f338a86b5a1	34
4142534445464748	90970b5d41dba4c0	23
4142435445464748	15477ed3856a5e2e	35
414243445546474e	069aa779e3e06492	29
41424344454e4748	14d478e9cb5c5747	32
4142434445465748	5ee074d94d408535	30
4142434445464758	8a80a15c40c4209e	26
6142434445464748	728526d74aa9643c	35
4162434445464748	91f29cc2cdc91b24	33
4142634445464748	e9eb31d98b8b22ad	25
4142436445464748	63d7e796ce5b60f5	31
4142434465464748	03eca522d0c0bbba	30
4142434445464768	fca938cb0bd6b4ff	25
ค่าเฉลี่ยระยะแฮมมิ่ง		29.79

ตารางที่ 8 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อข้อมูลเนื้อแท้ มีความแตกต่างกัน 1 บิต เมื่อใช้อัลกอริทึมไอเดส กรณีที่ 7

หมายเหตุ : ข้อมูลเนื้อแท้และข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัส ในตารางแสดงเป็นตัวเลขอยู่ในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 12 12 12 12
ข้อมูลออก แบ่งเป็นกลุ่มละ 8 8 8 8
คีย์สำหรับเข้ารหัสลับ : 0123456789abcdef

ข้อมูลเนื้อแท้	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
4142434445464748	073e1b3d1ce0d91c	
5142434445464748	93dcee0180081a3a	32
4152434445464748	1c1c8f86e27ec714	32
4142534445464748	7e616e840109f5e3	41
4142435445464748	606221b14ef743c6	32
414243445546474e	e68d10fb0cadef70	29
41424344454e4748	1e9855324927aca4	33
4142434445465748	a2fd8a36d1089b2f	29
4142434445464758	f6ce9976155f7b7e	30
6142434445464748	34570596890a69a2	35
4162434445464748	2dfe58435323529b	31
4142634445464748	1f1b7ad612d85445	28
4142436445464748	239478ca1350b052	32
4142434465464748	4cc1db5828c8a962	32
4142434445464768	e70eda5978152b03	30
ค่าเฉลี่ยระยะแฮมมิ่ง		31.86

ตารางที่ 9 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อข้อมูลเนื้อแท้ มีความแตกต่างกัน 1 บิต เมื่อใช้อัลกอริทึมไอเดส กรณีที่ 8

หมายเหตุ : ข้อมูลเนื้อแท้และข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัส ในตารางแสดงเป็นตัวเลขอยู่ในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 7 13 8 12 8
ข้อมูลออก แบ่งเป็นกลุ่มละ 4 9 6 8 5
คีย์สำหรับเข้ารหัสลับ : 0123456789abcdef

ข้อมูลเนื้อแท้	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
4142434445464748	cce24c047ddb7b48	
5142434445464748	617f090aa7d4cbc5	32
4152434445464748	0e05519438050cc8	31
4142534445464748	43330eee3f1532c7	31
4142435445464748	0437817ec0f37434	35
414243445546474e	cbfbf06dad4e3656	30
41424344454e4748	020e0e0a28be822a	32
4142434445465748	c09a813e6e6ee9d0	29
4142434445464758	01977a2e4575d18b	33
6142434445464748	d7f4d099ef592f6f	28
4162434445464748	8050ea350c3e6c9d	32
4142634445464748	8fc7d7a52f6e022c	30
4142436445464748	83ccd6f90247ab83	39
4142434465464748	06c6cc556acab1e1	24
4142434445464768	cee4ce776f11254e	23
ค่าเฉลี่ยระยะแฮมมิ่ง		30.64

ตารางที่ 10 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อข้อมูลเนื้อแท้
มีความแตกต่างกัน 1 บิต เมื่อใช้อัลกอริทึมไอเดส กรณีที่ 9

หมายเหตุ : ข้อมูลเนื้อแท้และข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัส ในตารางแสดงเป็นตัวเลข
อยู่ในรูปฐานสิบหก

ผลการทดสอบการเปลี่ยนแปลงของข้อมูลเข้ารหัส เมื่อคีย์สำหรับเข้ารหัสลับ
เปลี่ยนไป 1 บิต ของอัลกอริทึมเดสและอัลกอริทึมไอเดสกรณีต่าง ๆ

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 6 6 6 6 6 6 6 6
ข้อมูลออก แบ่งเป็นกลุ่มละ 4 4 4 4 4 4 4 4
ข้อมูลเนื้อแท้ : 4142434445464748

คีย์สำหรับเข้ารหัสลับ	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
0123456789abcdef	fa46606cfc0449cc	
1123456789abcdef	959828db89e821fe	36
0162456789abcdef	2f4cae58760b734e	28
0123656789abcdef	7074e1e8e7263ad1	25
0123454789abcdef	4469fe35e02a1ce8	33
0123456709abcdef	af62109fd1eba6ab	38
01234567898bcdef	146863875fdafcc8	34
0123456789ab8def	cbab75577ebafe02	36
0123456789abcd6f	12de892ad13dc7b8	31
0323456789abcdef	da07c23865d65b22	25
0127456789abcdef	8fbcf72d80f4b1cf	34
01234d6789abcdef	1deebc58c79fc7f3	37
0123456589abcdef	481bda81513e49d7	33
0123456781abcdef	fefd6d712939162a	35
0123456789afcdef	33bbcbcb30bc7471	40
ค่าเฉลี่ยระยะแฮมมิ่ง		33.21

ตารางที่ 11 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อคีย์สำหรับเข้ารหัสลับ มีความแตกต่างกัน 1 บิต โดยใช้อัลกอริทึมเดส

หมายเหตุ : ข้อมูลเนื้อแท้ ข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัสลับ ในตารางแสดงข้อมูลเป็นตัวเลขในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 5 5 5 5 5 5 5 5 8
ข้อมูลออก แบ่งเป็นกลุ่มละ 3 3 3 3 3 3 3 3 8
ข้อมูลเนื้อแท้ : 4142434445464748

คีย์สำหรับเข้ารหัสลับ	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
0123456789abcdef	9d96b959e1bc384f	
1123456789abcdef	f1cdfbbf1ca08336	37
0162456789abcdef	570f10931f6df6fe	36
0123656789abcdef	5194837073c4a5ca	27
0123454789abcdef	009d70bdd5063dd0	32
0123456709abcdef	bd5a32edf6a5e2c5	28
01234567898bcdef	4d70a6e154f86b1b	31
0123456789ab8def	5160162f4dd77f35	39
0123456789abcd6f	11344e10ef4be2d9	35
0323456789abcdef	ce7daede44d424ab	32
0127456789abcdef	be454b42c74f4e93	36
01234d6789abcdef	dcd197cf01bb1ac3	25
0123456589abcdef	eb2f95118e9281e4	35
0123456781abcdef	42d89885814fffa8	37
0123456789afcdef	53923aa204aae168	33
ค่าเฉลี่ยระยะแฮมมิ่ง		33.07

ตารางที่ 12 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อคีย์สำหรับเข้ารหัสลับ มีความแตกต่างกัน 1 บิต โดยใช้อัลกอริทึมไอเดส กรณีที่ 1

หมายเหตุ : ข้อมูลเนื้อแท้ ข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัสลับ ในตารางแสดงข้อมูลเป็นตัวเลขในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 6 6 6 6 12 12
ข้อมูลออก แบ่งเป็นกลุ่มละ 4 4 4 4 8 8
ข้อมูลเนื้อแท้ : 4142434445464748

คีย์สำหรับเข้ารหัสลับ	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
0123456789abcdef	aeea42ebc1b2f976	
1123456789abcdef	ffc8ed5aba9d6cf5	33
0162456789abcdef	1724ca83ef1a55ec	30
0123656789abcdef	1981a8749d0ce7d9	42
0123454789abcdef	6410d9e539faa1e4	31
0123456709abcdef	807b77234e6cafbd	34
01234567898bcdef	01c88f497a09bff9	36
0123456789ab8def	c19b648706159de1	35
0123456789abcd6f	4d84da1c870d2d1c	38
0323456789abcdef	95a10fd811a29483	32
0127456789abcdef	d549c9bc7a05afcd	41
01234d6789abcdef	43f3f5dd35d0d9f2	30
0123456589abcdef	4e99c198babffaf6	28
0123456781abcdef	cf060d950fdf550c	38
0123456789afcdef	e58f9fcf562f7f0c	34
ค่าเฉลี่ยระยะแฮมมิ่ง		34.43

ตารางที่ 13 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อคีย์สำหรับเข้ารหัสลับ มีความแตกต่างกัน 1 บิต โดยใช้อัลกอริทึมไอเดส กรณีที่ 2

หมายเหตุ : ข้อมูลเนื้อแท้ ข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัสลับ ในตารางแสดงข้อมูลเป็นตัวเลขในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 7 7 7 7 7 7 6
ข้อมูลออก แบ่งเป็นกลุ่มละ 5 5 5 5 4 4 4
ข้อมูลเนื้อแท้ : 4142434445464748

คีย์สำหรับเข้ารหัสลับ	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
0123456789abcdef	e21892969e587202	
1123456789abcdef	56afb3feb6390129	29
0162456789abcdef	75c3e19ec5c20da3	36
0123656789abcdef	ee5867ea83de425f	28
0123454789abcdef	fb7f0ff0d107b943	35
0123456709abcdef	94d82ef7ba5fa64f	28
01234567898bcdef	7773442cd1e22837	37
0123456789ab8def	9bb92e16447afafd	31
0123456789abcd6f	20c3779349ab80df	39
0323456789abcdef	6de67c1449caaef2	38
0127456789abcdef	834cfff8b366d12f	33
01234d6789abcdef	c8808c7703bb0a46	30
0123456589abcdef	d1b6b05e1c05426c	28
0123456781abcdef	2e43955333445918	31
0123456789afcdef	3bac8bf6c86ce0be	29
ค่าเฉลี่ยระยะแฮมมิ่ง		32.29

ตารางที่ 14 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อคีย์สำหรับเข้ารหัสลับ มีความแตกต่างกัน 1 บิต โดยใช้อัลกอริทึมไอเดส กรณีที่ 3

หมายเหตุ : ข้อมูลเนื้อแท้ ข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัสลับ ในตารางแสดงข้อมูลเป็นตัวเลขในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 8 8 8 8 8 8
ข้อมูลออก แบ่งเป็นกลุ่มละ 6 6 6 6 4 4
ข้อมูลเนื้อแท้ : 4142434445464748

คีย์สำหรับเข้ารหัสลับ	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
0123456789abcdef	32499389f539f680	
1123456789abcdef	baad4e6423ae6fce	36
0162456789abcdef	06db60b4fe28826c	31
0123656789abcdef	b6394fc736480090	29
0123454789abcdef	5eb6caed5c7f359f	35
0123456709abcdef	c884923c9220e8e3	33
01234567898bcdef	3b5c58972b5c0034	34
0123456789ab8def	4ad3606f7f4427cd	36
0123456789abcd6f	fb433d2dc544b816	30
0323456789abcdef	ac4bc8b7c1b9260f	28
0127456789abcdef	b311569f24b01e55	28
01234d6789abcdef	39320bf69aeb199e	40
0123456589abcdef	0e9657cb957dbae2	26
0123456781abcdef	56f12555d2947ed2	31
0123456789afcdef	4fd049699a3ffac9	31
ค่าเฉลี่ยระยะแฮมมิ่ง		32.00

ตารางที่ 15 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อคีย์สำหรับเข้ารหัสลับ มีความแตกต่างกัน 1 บิต โดยใช้อัลกอริทึมไอเดส กรณีที่ 4

หมายเหตุ : ข้อมูลเนื้อแท้ ข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัสลับ ในตารางแสดงข้อมูลเป็นตัวเลขในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 5 6 10 8 9 10
ข้อมูลออก แบ่งเป็นกลุ่มละ 3 4 7 5 6 7
ข้อมูลเนื้อแท้ : 4142434445464748

คีย์สำหรับเข้ารหัสลับ	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
0123456789abcdef	07cdae1ba8d16ee2	
1123456789abcdef	9d8ea0366c0c82e8	30
0162456789abcdef	294d38a1ccab9507	34
0123656789abcdef	dfe73e5416c6fd19	35
0123454789abcdef	83b832dc0d2cda46	34
0123456709abcdef	251abf315a4155d7	29
01234567898bcdef	26d592ca3d8ffc9e	29
0123456789ab8def	6cee3531f6d7f18e	33
0123456789abcd6f	8fcc75476268623b	29
0323456789abcdef	24efd3070b178a06	30
0127456789abcdef	563674b7d70b87c0	38
01234d6789abcdef	bc00a88db293c90c	33
0123456589abcdef	44874870b85b4459	29
0123456781abcdef	3e9f24bfdb63354c	32
0123456789afcdef	0bdf0635427b1419	32
ค่าเฉลี่ยระยะแฮมมิ่ง		31.93

ตารางที่ 16 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อคีย์สำหรับเข้ารหัสลับ มีความแตกต่างกัน 1 บิต โดยใช้อัลกอริทึมไอเดส กรณีที่ 5

หมายเหตุ : ข้อมูลเนื้อแท้ ข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัสลับ ในตารางแสดงข้อมูลเป็นตัวเลขในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 7 10 12 8 11
ข้อมูลออก แบ่งเป็นกลุ่มละ 5 6 8 6 7
ข้อมูลเนื้อแท้ : 4142434445464748

คีย์สำหรับเข้ารหัสลับ	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
0123456789abcdef	9faca37cf9418a21	
1123456789abcdef	3afc366a49cf4a8a	27
0162456789abcdef	e5f714ff8b7a69ae	38
0123656789abcdef	8934bd7341c6156b	31
0123454789abcdef	81bd43b1ab9c4874	30
0123456709abcdef	124f8fc3aa498471	29
01234567898bcdef	1c54257594946a0f	30
0123456789ab8def	22276d135b6b2e8d	34
0123456789abcd6f	a7fa80e9c9ab44cf	32
0323456789abcdef	36e23d01c8216663	31
0127456789abcdef	c3f2b10ee289adad	29
01234d6789abcdef	513a890ba09507e5	33
0123456589abcdef	06590b80347fc6b8	36
0123456781abcdef	a1be9b2d5c52f326	28
0123456789afcdef	ce0eb63392815047	30
ค่าเฉลี่ยระยะแฮมมิ่ง		31.29

ตารางที่ 17 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อคีย์สำหรับเข้ารหัสลับ มีความแตกต่างกัน 1 บิต โดยใช้อัลกอริทึมไอเดส กรณีที่ 6

หมายเหตุ : ข้อมูลเนื้อแท้ ข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัสลับ ในตารางแสดงข้อมูลเป็นตัวเลขในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 12 8 6 10 12
ข้อมูลออก แบ่งเป็นกลุ่มละ 8 5 4 7 8
ข้อมูลเนื้อแท้ : 4142434445464748

คีย์สำหรับเข้ารหัสลับ	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
0123456789abcdef	2fca89c940db84eb	
1123456789abcdef	98838b8c0ef1f591	29
0162456789abcdef	958eb6eb8173b40b	26
0123656789abcdef	eb32c56402e5861f	29
0123454789abcdef	965bd8804e921304	32
0123456709abcdef	9f4c320d4b6a04f8	26
01234567898bcdef	d9d9b0a7c85f36f8	29
0123456789ab8def	f379fda1cb02bd10	37
0123456789abcd6f	36cd83a4830fc199	28
0323456789abcdef	670e258c8796577a	29
0127456789abcdef	54e078b1c25b0de8	26
01234d6789abcdef	be20982387d10911	32
0123456589abcdef	223464b905e28170	33
0123456781abcdef	9b393005408858e7	30
0123456789afcdef	670b4c63871265da	29
ค่าเฉลี่ยระยะแฮมมิ่ง		29.64

ตารางที่ 18 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อคีย์สำหรับเข้ารหัสลับ มีความแตกต่างกัน 1 บิต โดยใช้อัลกอริทึมไอเดส กรณีที่ 7

หมายเหตุ : ข้อมูลเนื้อแท้ ข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัสลับ ในตารางแสดงข้อมูลเป็นตัวเลขในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 12 12 12 12
ข้อมูลออก แบ่งเป็นกลุ่มละ 8 8 8 8
ข้อมูลเนื้อแท้ : 4142434445464748

คีย์สำหรับเข้ารหัสลับ	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
0123456789abcdef	073e1b3d1ce0d91c	
1123456789abcdef	58fc5b17bf4f16d4	32
0162456789abcdef	c8d3df83211af861	40
0123656789abcdef	9799b94e4ccfb3a5	31
0123454789abcdef	c9a4058ec37e0ef1	42
0123456709abcdef	282317cbcbb7e061	38
01234567898bcdef	cf6df7cb68a54d35	31
0123456789ab8def	5a9ee3dcd25e4b2e	33
0123456789abcd6f	b382d5a5feaa15fc	31
0323456789abcdef	2be937d0f71d0007	40
0127456789abcdef	6f745850903d4b91	30
01234d6789abcdef	1ed4defe8e6f598e	28
0123456589abcdef	9e5d1b84ddf2bcb0	26
0123456781abcdef	4cdb8430af3e2a69	40
0123456789afcdef	381b0456f2759a37	36
ค่าเฉลี่ยระยะแฮมมิ่ง		34.14

ตารางที่ 19 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อคีย์สำหรับเข้ารหัสลับมีความแตกต่างกัน 1 บิต โดยใช้อัลกอริทึมไอเดส กรณีที่ 8

หมายเหตุ : ข้อมูลเนื้อแท้ ข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัสลับ ในตารางแสดงข้อมูลเป็นตัวเลขในรูปฐานสิบหก

ข้อมูลเข้า แบ่งเป็นกลุ่มละ 7 13 8 12 8
ข้อมูลออก แบ่งเป็นกลุ่มละ 4 9 6 8 5
ข้อมูลเนื้อแท้ : 4142434445464748

คีย์สำหรับเข้ารหัสลับ	ข้อมูลเข้ารหัส	ระยะแฮมมิ่ง
0123456789abcdef	cce24c047ddb7b48	
1123456789abcdef	8ffb9835285a9528	27
0162456789abcdef	01200b71e58d4c73	34
0123656789abcdef	cc98f6fff9a710dc	32
0123454789abcdef	8d0ef7d5e4ea544c	30
0123456709abcdef	c1fc0a0c1d370c79	27
01234567898bcdef	cb38e872ae0f67fc	32
0123456789ab8def	c774def4d8986923	28
0123456789abcd6f	4b759d20c85dcc72	33
0323456789abcdef	04448ca6e2aa2bfd	29
0127456789abcdef	445b102c8dd6fce1	28
01234d6789abcdef	084ce4d14fc20172	31
0123456589abcdef	c54b501598248604	34
0123456781abcdef	c0403ecf50c067f3	31
0123456789afcdef	8ef6729eff837ff7	26
ค่าเฉลี่ยระยะแฮมมิ่ง		30.14

ตารางที่ 20 แสดงการเปลี่ยนแปลงของข้อมูลเข้ารหัสเมื่อคีย์สำหรับเข้ารหัสลับมีความแตกต่างกัน 1 บิต โดยใช้อัลกอริทึมไอเดส กรณีที่ 9

หมายเหตุ : ข้อมูลเนื้อแท้ ข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัสลับ ในตารางแสดงข้อมูลเป็นตัวเลขในรูปฐานสิบหก

ประวัติผู้เขียน

นางสาว สมศรี จตุรพิธพรชัย เกิดเมื่อวันที่ 5 พฤษภาคม พ.ศ. 2502 ที่กรุงเทพมหานคร สำเร็จการศึกษาศิลปศาสตรบัณฑิต (สาขาสถิติ) จากคณะศิลปศาสตร์ มหาวิทยาลัยธรรมศาสตร์ เมื่อปี พ.ศ. 2524 ปัจจุบันรับราชการในตำแหน่ง เจ้าหน้าที่ระบบงานคอมพิวเตอร์ สังกัดสำนักคอมพิวเตอร์ มหาวิทยาลัยมหิดล