





Tel: 0845 519 0154

+44(0)1276 510724

[info@hdencrypt.com](mailto:info@hdencrypt.com)

## Hawthorne Davies Limited

The position of character 65 is highlighted.

The question is: What happens to the distribution of the decrypted AAAA.TXT when the Master Key contains a minimal alteration? The immediate effect is that, thanks to the powerful FUSION sub-routine, the primitives that form the session key are totally altered:

**Alteration point = 5439 Hex number at 5439 = 3 altered to 2**

```
F11B13F18205DBDFAF7F13690E928724355DFD08E235E4664F8DB150D0339CD49473A00A153A0
CCD883B0ED055951EF6279B379A04F382630B8F6AFA11C86D4E30A0FAAEF7E8608BCA29644C179
7053D77BE30E4F1463B42D9D828AA5AA9A03514FECD01CB2C1E9DFC87C3197770898BFD22869A
19633E82B97437DC0EE58B1400AD7396C8F2414F7E3AABD4D6AC3373F5367AD515FC30F45C7C5
AFFD0551761C9730C0F92ECA4D06F9AEC68D4E91F1D7B42E833B4EE1429496B2727C503D1DADBE
5B7096DAFFA0E1CF9BDBBE513B12128EFA95749E8E4689A6E2795FCD50278B41FE886825B263
F6E7AA7262C4F6B053901BEE169F99B701FCC085998B7D91CBFC8CF648B7EBF41BE70CA0851659
7A82B4160324540F070E5E123A997898F2E4108C78E0121FA1EF75F1E4E8DFE81D1A47259F8B0B
B2BC2F31B2B114288ACD889C36863689C377D694F8FAA0A40AB8FDDC809469B181F4F6AC3D4F
110407680136765DD6A826A35B05E75CFD0F3F6F6656F8E66C1209150FC7D63A4BFD395413397E
5E059CDBAC47A9FC6A012BEB9BF3C807AFC5719914E94FB6FD79A63FB5E866700E4C6EAA357E
CEECBD77434B0730725827401053DD7525FDA191EFC3BE18A692B54856B78BE99B76F147790B0F
6674BF6F0ADF8374FA8D92DF32E2A55EB7B7D2B1BE397E30B104CC4BBB75B99E0E589F5B0A4C
6A39710D96B2C07452F15A8DD90DEC9C9D9BB3332C98929A84D0BC979342733B705FE8218C8780
F6A9504ED39200BC1C4529F4B8F03F1F339C568797F54E068883D340BBB5074E1E463DD14D2D9
41DC88FF1ACD3B520E180C831F96F9AF2E1E335EF8D05628954AD0A1300C2102AD8E4AF22F960C
18A908DC8F406592760F344A535C06B841F8CADF2A687DDCB629178AE0CC5FF99E0E65CF5338CA
640A37495F6FFB436D772358774ED7BE15DF2375A1DD61F4B9B9696758762B96FDA9D4189B6613
0D682768A500A8ECD91A409489945FC2179EE511D58BE806281977FEADACD97E5A68BA348D60B
608C4A0AA559271EE0B0A2D733CD59678281D00D42A2F6195ADDE0
```

The resulting distribution within the decrypted AAAA.TXT of ASCII characters in the range 0 - 255 is:

**Alteration point = 5439 Hex number at 5439 = 3 altered to 2**

```
80 107 90 88 109 111 94 110 106 90 97 97 104 93 75 105 93 104
93 90 102 109 114 91 101 85 109 89 112 104 84 121 101 105 113
116 112 108 102 111 89 110 105 91 111 96 96 106 99 92 139 87
92 96 77 91 86 105 112 108 112 97 90 104 99 92 101 101 102 99
101 107 106 83 97 97 113 94 104 96 102 93 107 111 122 105 98
82 102 95 102 97 112 85 113 87 107 72 90 104 102 98 110 83 98
100 87 91 93 112 93 96 107 109 99 111 90 107 89 88 117 105
111 95 119 106 124 100 94 116 88 97 117 77 110 101 101 94 97
97 88 113 99 88 91 117 112 85 108 87 99 112 108 105 110 78
118 107 116 94 108 80 96 118 100 107 100 90 116 104 90 90 116
88 74 98 106 104 109 84 106 108 98 88 89 101 105 99 117 103
116 103 102 93 87 87 103 114 97 112 102 108 106 96 112 109 107
95 89 98 94 100 78 98 79 92 107 97 110 114 94 116 105 92 107
104 104 97 108 84 104 94 88 111 115 103 97 107 81 96 100 97
87 96 96 97 99 83 111 87 91 102 89 99 100 104
```

Repeating the test for a second minimal alteration produces a distribution of ASCII values in the decrypted version of AAAA.TXT as follows:

**Alteration point = 461 Hex number at 461 = 6 altered to 7**

```
98 89 106 108 102 101 87 103 106 110 115 99 89 109 104 101 106
97 111 99 88 103 98 100 103 115 106 92 103 104 103 95 90 114
90 97 115 96 86 104 95 109 91 99 101 81 117 99 112 106 90 108
109 110 90 95 99 82 106 97 104 125 103 108 111 91 106 108 105
86 96 89 117 83 95 97 88 101 93 97 104 96 107 108 118 93 106
102 85 114 97 83 104 100 77 100 104 104 89 104 93 95 103 97
110 103 106 108 85 99 108 103 90 114 103 91 114 85 95 88 99
90 108 91 102 105 97 88 102 100 98 110 110 103 105 88 99 93
111 98 94 96 108 116 112 88 88 104 102 104 111 119 93 107 91
95 97 117 99 108 107 119 101 101 97 111 78 101 84 90 99 105
105 84 124 84 96 112 104 101 87 104 116 99 94 89 88 116 100
91 93 93 77 102 113 77 101 93 109 96 108 92 78 102 91 91 116
99 84 103 113 112 108 95 102 112 104 96 112 85 126 94 105 100
121 82 109 97 104 103 92 100 101 97 116 106 106 83 107 93 99
101 96 106 102 105 85 91 110 76 89 89 85 103 110 95
```

It is clear that each of the above alterations result in a completely unintelligible decrypt.



Tel: 0845 519 0154

+44(0)1276 510724

[info@hdencrypt.com](mailto:info@hdencrypt.com)

## Hawthorne Davies Limited

In the interests of certainty we now introduce "Monte Carlo" methods. We do these by writing a program which randomises the point of alteration in the Master Key and also randomises the degree of alteration at the selected point. The results are conclusive. There is no redundancy in the Master Key:

1. Point of alteration 1-6144
2. Hex character at the point of alteration
3. Replacement hex character
4. Frequency of "A" in the resulting decrypted file

5910	1	0	90	5887	1	0	102	1103	A	B	112
5448	6	7	113	626	C	D	115	1074	8	7	105
407	0	1	99	4582	6	5	101	3845	0	1	90
5478	8	8	25600	1217	E	F	82	3837	9	8	102
726	6	7	98	4215	B	A	104	3559	D	D	25600
3179	C	B	85	2046	3	4	108	2256	8	9	104
1639	6	7	101	5847	7	6	98	4359	D	E	102
5586	A	A	25600	1141	1	2	98	3387	8	7	121
1770	E	F	97	4786	E	E	25600	2922	A	B	101
3504	D	C	99	40	2	3	100	2674	5	6	109
2840	4	5	101	3352	D	D	25600	2029	7	6	89
903	9	A	95	1967	A	9	96	1328	5	5	25600
4465	2	3	80	607	2	2	25600	1056	6	7	81
1228	1	2	95	5399	C	D	98	662	9	9	25600
1562	3	2	89	2054	6	7	124	299	F	0	84
2507	2	1	91	5317	A	9	90	4108	E	F	98
134	6	6	25600	142	0	1	105	686	B	A	115
1130	4	3	99	2130	5	5	25600	2333	0	F	97
3477	3	2	95	5999	E	F	83	5019	5	5	25600
4986	2	1	92	5805	A	9	113	2909	C	B	82
4869	0	1	82	5824	9	9	25600	2332	C	C	25600
360	3	3	25600	328	8	7	98	68	8	7	100
5435	D	E	99	1219	5	4	91	2930	A	B	105
4281	E	F	107	4748	8	8	25600	1298	C	C	25600
5585	7	7	25600	5289	8	9	25600	1234	D	C	112
2772	4	4	25600	2649	5	4	111	171	8	7	99
3189	A	B	92	2482	3	2	100	1608	6	6	25600
2024	9	9	25600	5397	2	2	25600	6011	8	7	100
3798	6	7	106	680	4	5	112	2709	4	4	25600
5959	2	1	118	2211	0	F	111	1361	4	5	108
5580	5	6	107	3300	D	E	95	3989	9	9	25600
4960	8	9	103	282	7	8	93	555	9	A	116
2995	E	F	91	2118	1	0	93	3458	D	C	107
2529	4	5	97	89	E	F	79	5187	F	F	25600
2744	0	0	25600	2213	5	4	95	821	2	2	25600
888	A	B	100	5094	8	7	81	326	F	E	89
595	7	6	115	4779	C	B	95	3998	3	4	99
365	7	8	98	2251	C	B	95	2714	A	B	96
4604	2	1	115	3772	8	8	25600	4690	8	7	100
4285	C	B	97	5497	E	D	100				
2372	E	F	125	2510	0	1	88	1	B	C	99
2971	C	D	93	2471	E	D	88	6144	C	D	90