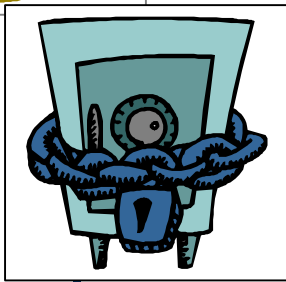
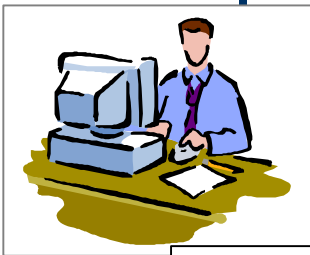


Tech Juris

A White Paper prepared for
Asian School of Cyber Laws
www.asianlaws.org



Skipjack

ASCL White Papers can be downloaded from:
www.asianlaws.org/whitepapers

Tech Juris
The Technology Lawyers
www.techjuris.com

Skipjack, the originally secret algorithm associated with the infamous Clipper chip, was declassified on Tuesday, June 23, 1998, and appeared as a .PDF document at the NIST web site the following morning.

The basic round type of Skipjack forms another alternative, alongside those offered by SAFER and IDEA, to the Feistel round structure seen in DES, LUCIFER and Blowfish, among other block ciphers.

In each round, one of four quarters of the block is subjected to four Feistel rounds on a small scale, and one other quarter is modified by being XORed with the round number and the quarter that went through the mini-Feistel cipher, either before or after that step. No bit transposes are required in Skipjack, making it efficient to implement on a general-purpose computer.

Skipjack has 32 rounds. These rounds are of two types, A and B. A type A round proceeds as follows:

The first quarter of the block (called W1) is enciphered by the "G permutation", which is actually a four-round Feistel cipher. The result, and the round number (where round numbers go from 1 through 32), is XORed with the fourth quarter of the block (W4). Then each quarter of the block is moved to the next position; W1 to W2, W2 to W3, W3 to W4, and W4 back to W1.

A type B round proceeds as follows:

The second quarter of the block (W2) is XORed with the round number and the first quarter of the block (W1). Then the first quarter of the block is enciphered by the "G permutation". Again, each quarter of the block is moved to the next position; W1 to W2, W2 to W3, W3 to W4, and W4 back to W1.

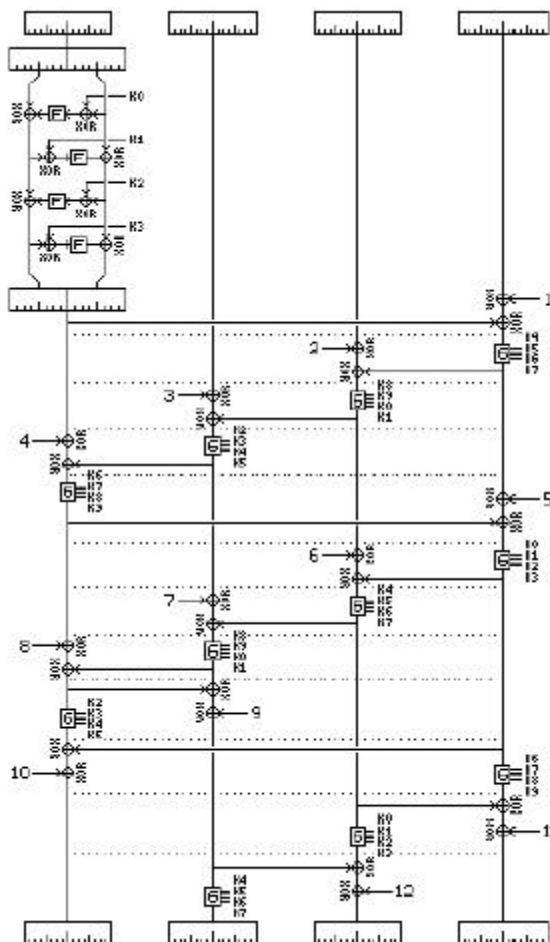
The rotation of quarters of the block is not omitted after the last round. The 32 rounds of Skipjack consist of eight type A rounds, eight type B rounds, eight type A rounds, and eight type B rounds. Note that by having a type A round first, and a type B round last, the form of the first quarter on the "inside" is XORed with one of the other quarters in the first and last rounds.

Permutation G is a four-round Feistel cipher, involving dividing its 16-bit input into two 8-bit halves. Like DES, the left half of the block is not changed in each round, but acts as input to the f-function, the output of which is XORed to the right half. Unlike DES, the two halves are swapped after the last round (as the algorithm has only four rounds, all four iterations of the f-function can be illustrated, going alternately from right to left, and then from left to right; in that form, no swaps at all are required).

The f-function of the G permutation is as simple as one might expect for an f-function only 8 bits wide: the input is first XORed with the current round's sub key, and then the result is substituted according to a lookup table, called F.

The sub keys for G, each one byte long, are simply four consecutive bytes of the 80-bit key. The first four bytes are used in the first round, the next four bytes in the second, the last two bytes followed by the first two bytes in the third, and so on.

The operation of Skipjack may be made clearer by the following diagram, which illustrates the first 12 rounds of Skipjack. The first round, of type A, is shown with the G function illustrated in full. The next seven rounds, also of type A, are shown with the G function indicated by a box marked with a G. Then the last four of the twelve rounds shown, of type B, are showed the same way. There are dotted lines dividing the rounds in the diagram.



Instead of rotating the quarters of the block, the functions move between columns; since the last rotation is not skipped, this illustration will show, if continued to include all 32 rounds, the quarters ending up in their proper places without any final rotation being required.

The S-box of Skipjack, called F, which is the heart of the f-function of the Feistel mini-cipher that is the G permutation, is as follows:

```
a3 d7 09 83 f8 48 f6 f4 b3 21 15 78 99 b1 af f9
e7 2d 4d 8a ce 4c ca 2e 52 95 d9 1e 4e 38 44 28
0a df 02 a0 17 f1 60 68 12 b7 7a c3 e9 fa 3d 53
96 84 6b ba f2 63 9a 19 7c ae e5 f5 f7 16 6a a2
39 b6 7b 0f c1 93 81 1b ee b4 1a ea d0 91 2f b8
55 b9 da 85 3f 41 bf e0 5a 58 80 5f 66 0b d8 90
35 d5 c0 a7 33 06 65 69 45 00 94 56 6d 98 9b 76
97 fc b2 c2 b0 fe db 20 e1 eb d6 e4 dd 47 4a 1d
42 ed 9e 6e 49 3c cd 43 27 d2 07 d4 de c7 67 18
89 cb 30 1f 8d c6 8f aa c8 74 dc c9 5d 5c 31 a4
70 88 61 2c 9f 0d 2b 87 50 82 54 64 26 7d 03 40
34 4b 1c 73 d1 c4 fd 3b cc fb 7f ab e6 3e 5b a5
ad 04 23 9c 14 51 22 f0 29 79 71 7e ff 8c 0e e2
0c ef bc 72 75 6f 37 a1 ec d3 8e 62 8b 86 10 e8
08 77 11 be 92 4f 24 c5 32 36 9d cf f3 a6 bb ac
5e 6c a9 13 57 25 b5 e3 bd a8 3a 01 05 59 2a 46
```

or, in decimal form,

```
163 215 9 131 248 72 246 244 179 33 21 120 153 177 175 249
231 45 77 138 206 76 202 46 82 149 217 30 78 56 68 40
10 223 2 160 23 241 96 104 18 183 122 195 233 250 61 83
150 132 107 186 242 99 154 25 124 174 229 245 247 22 106 162
57 182 123 15 193 147 129 27 238 180 26 234 208 145 47 184
85 185 218 133 63 65 191 224 90 88 128 95 102 11 216 144
53 213 192 167 51 6 101 105 69 0 148 86 109 152 155 118
151 252 178 194 176 254 219 32 225 235 214 228 221 71 74 29
66 237 158 110 73 60 205 67 39 210 7 212 222 199 103 24
137 203 48 31 141 198 143 170 200 116 220 201 93 92 49 164
112 136 97 44 159 13 43 135 80 130 84 100 38 125 3 64
52 75 28 115 209 196 253 59 204 251 127 171 230 62 91 165
173 4 35 156 20 81 34 240 41 121 113 126 255 140 14 226
12 239 188 114 117 111 55 161 236 211 142 98 139 134 16 232
8 119 17 190 146 79 36 197 50 54 157 207 243 166 187 172
94 108 169 19 87 37 181 227 189 168 58 1 5 89 42 70
```

This was double-checked by looking at the inverse of this S-box generated by the same program that converted what was typed from hexadecimal to decimal, as the S-box is a straight permutation of the numbers from 0 to 255. In the original document in its electronic form, lowercase c and e are sometimes difficult to distinguish.

For decipherment, a corresponding deciphering round replaces each round, and these rounds are, of course, executed in the reverse of the enciphering order.

The deciphering equivalent of a type A round is as follows:

The first quarter, W1, is XORed with W2 and the round number (rounds now counting down

from 32 to 1). Then the second quarter, W2, is subjected to the inverse of the G permutation. Then, each quarter is moved to the position of the preceding one; W1 to W4, W2 to W1, W3 to W2, and W4 to W3.

The deciphering equivalent of a type B round is the following:

The second quarter, W2, is subjected to the inverse of the G permutation. The third quarter, W3, is then XORed with the round number and the changed value of W2. Again, each quarter is moved to the position of the preceding one; W1 to W4, W2 to W1, W3 to W2, and W4 to W3.

The deciphering equivalent of the G permutation involves using the four sub keys in reverse order – and reversing the roles of the right and left halves of the 16-bit quarter block.



OUR SERVICES

Information Security

- Training
- Consultancy
- White papers
- Workshops

Technology Law

We provide training, consultancy, workshops, and white papers in the following areas of law:

- Media Laws
- Semi-conductor Law
- Intellectual Property Law
- PKI Law
- Cyber Law
- Drafting
- Software valuation
- Audits
- Arbitration
- E-contracts

In addition, we conduct a Diploma course in Information Technology Law.

Cyber Crime Investigation

- Training
- Consultancy
- Search and seizure operations
- White papers
- Certified Courses

CONTACT US

Regd. Office

6, Rajas, Above IDBI, Pashan Road, Pune 411008

Ph: 91 20 5890894 / 95

Fax: 91 20 5675600

Email: info@asianlaws.org

URL: www.asianlaws.org

This White Paper is provided for general information only. Neither Asian School of Cyber Laws (ASCL) nor Tech Juris (TJ) makes any warranty, express or implied, to the accuracy of the contents of these White Papers. Although all reasonable care and caution is taken while preparing these White Papers, errors and omissions may occur and neither ASCL nor TJ will be liable for any direct, indirect, special, incidental or consequential damages or loss (including damages for loss of business, loss of profits, or the like) arising directly or indirectly from the use of information contained in this White Paper.