Attack on first key exchange protocol.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Matrix order | Max cycle length searched | Max terms searched | N | N successfully attacked | Max occurring cycle | Max terms needed |
| 30 | 20 | 2000 | 1000 | 1000 (100%) | 14 | 1282 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |