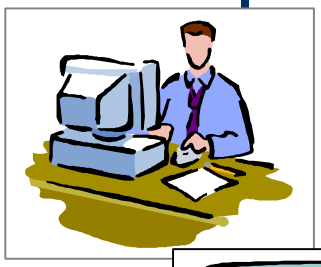
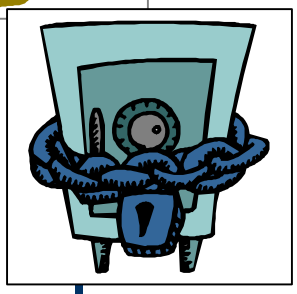
Tech Juris

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





The IDEA Algorithm

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

Tech Juris
The Technology Lawyers
www.techjuris.com

ASCL-WP-IS-Tec-Algo-04

IDEA is best known as a component of PGP. It is a block cipher, which uses a 128-bit length key to encrypt successive 64-bit blocks of plaintext. The procedure is quite complicated using sub keys generated from the key to carry out a series of modular arithmetic and XOR operations on segments of the 64-bit plaintext block. The encryption scheme uses a total of fifty-two 16-bit sub keys. These are generated from the 128-bit sub key as follows:

- The 128-bit key is split into eight 16-bit keys, which are the first eight sub keys.
- The digits of the 128-bit key are shifted 25 bits to the left to make a new key, which is split into the next eight 16-bit sub keys.

The second step is repeated until the fifty-two sub keys have been generated.

The encryption involves modular multiplication with a modulus of ((2^16)+1) and addition with a modulus of (2^16). The 64-bit plaintext block is split into four 16-bit segments, which we'll call p1, p2, p3 and p4. The sub keys are s1, s2, s3, s4 ....s52.

The encryption consists of eight rounds with each round involving the following steps:

```
p1 x s1 --> d1
p2 + s2 --> d2
p3 + s3 --> d3
p4 x s4 --> d4
d1 XOR d3 --> d5
d2 XOR d4 --> d6
d5 x s5 --> d7
d6 + d7 --> d8
d8 x s6 --> d9
d7 + d9 --> d10
d1 XOR d9  --> d11
d3 XOR d9  --> d12
d2 XOR d10 --> d13
d4 XOR d10 --> d14
```

After this process, the output blocks d12, d13 are exchanged so that d11, d13, d12 and d14 are used as input to the next round (in that order) along with the next 6 sub keys, s7 to s12. This procedure is followed for eight rounds in total giving four output blocks, which can be called e1, e2, e3 and e4. Four more steps using the last four sub keys complete the encryption:

```
e1 x s49 --> c1
e2 + s50 --> c2
e3 + s51 --> c3
e4 x s52 --> c4
```

Note: for the purposes of the algorithm, a key of all zeros is defined as being equal to 2^16, for modular multiplication steps.

The final four output blocks, c1 to c4, are re-attached to form a 64-bit block of the cipher text.

The whole process is repeated for successive 64-bit blocks of plaintext until all of the plaintext has been encrypted. Decryption uses exactly the same sequence of operations of successive 64-bit blocks of the cipher text, but with a different set of sub keys. The decryption sub keys are worked out from the encryption sub keys being either multiplicative or additive inverses of them. The decryption sub keys (relative to the encryption sub keys s1 to s52) are shown in the table below:

1st round	s49*	s50#	s51#	s52*	s47	s48
2nd round	s43*	s45#	s44#	s46*	s41	s42
3rd round	s37*	s39#	s38#	s39*	s35	s36
4th round	s31*	s33#	s32#	s34*	s29	s30
5th round	s25*	s27#	s26#	s28*	s23	s24
6th round	s19*	s21#	s20#	s22*	s17	s18
7th round	s13*	s15#	s14#	s16*	s11	s12
8th round	s7*	s9#	s8#	s10*	s5	s6
Final transformation.....	s1*	s2#	s3#	s4*		

```
sXX* = multiplicative inverse of sXX modulus ((2^16)+1)
sXX# = additive inverse of sXX modulus (2^16)
```

[NOTE: A sub key with all bits zero is its own multiplicative inverse in this algorithm]

Asian School of Cyber Laws

Pune | Bangalore | Kolkata | Nagpur

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