IDEA (International Data Encryption Algorithm).

1). It is a symmetric-key block cipher.

2). The algorithm was intended as a replacement for the DES. in 1991.

3). It operates on 64-bit blocks using a 128-bit key.

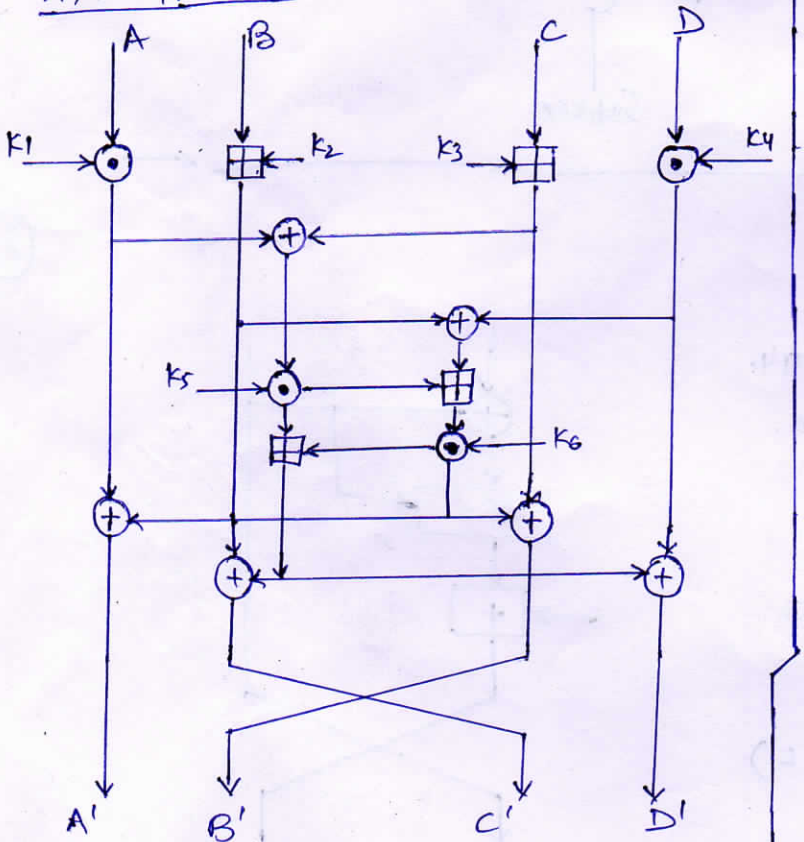
4). It consists of a series of eight identical transformations (a round) and an output transformation (a half round).

5). Following operations performed in IDEA:
   a) Bitwise X-OR ($\oplus$)
   b) Addition modulo 2^{16}. ($\boxplus$)
   c) Multiplication modulo $2^{16}+1$ ($\odot$)

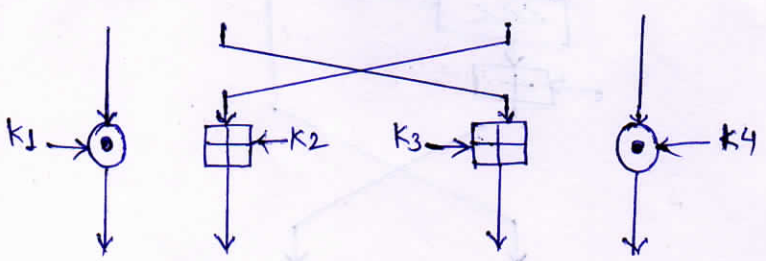
Subkey Generation

- The 128-bit key of IDEA is taken as the first eight subkeys K(1) to K(8).
- The next eight subkeys are obtained, after a 25-bit circular left shift.

An Encryption Round



Half Round



6). Each round uses six 16-bit subkeys, while the half round uses four, a total of 52 for 8.5 rounds.

7). Multiplication by zero always produces zero and is not invertible. Multiplication modulo n is also not invertible whenever it is by a number which is not relatively prime to n. The way multiplication is used in IDEA, it is necessary that it be always invertible.

So no. 65537 $(2^{16}+1)$ is a prime

$2^8+1 = 257$ is a prime

$2^4+1 = 17$ is a prime.

DESCRIPTION

Four quarters of plaintext A, B, C, D.

52 subkeys K(1) to K(52).

* Before round 1

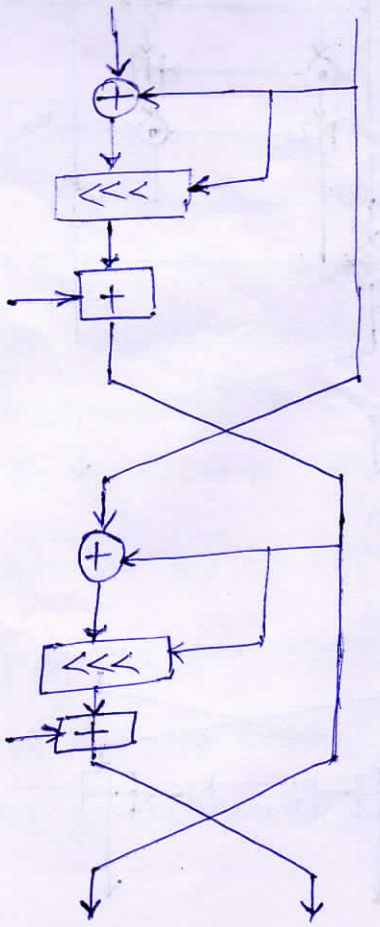
Multiply A by K(1), Add K(2) to B, Add K(3) to C, Multiply D by K(4).

* Round 1 proper

→ Calculate A XOR C (call it E)
   B XOR D (call it F).
→ Multiply E by K(5). Add new value of E to F.
→ Multiply new value of F by K(6). Add the result to E.
→ Change both A and C by XORing F.
   Change both B and D by XORing E.
→ Swap B and C.

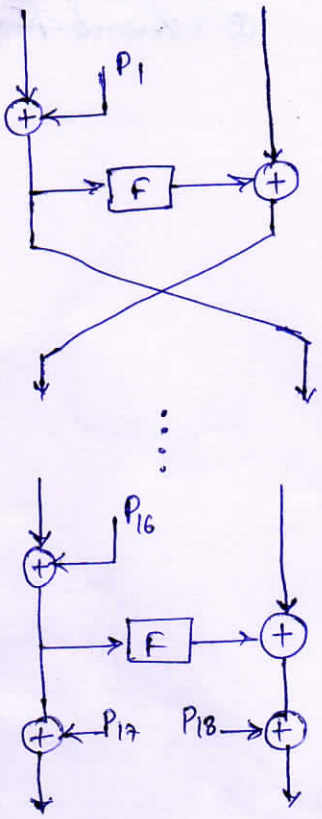
RC5 :-

1) It is a Symmetric block cipher.
2) Designed by Ronald Rivest in 1994.
3) RC stands For "Rivest Cipher" or. "Ron's Code".
4) Key size = 0 to 2040 bits.
   Block size = 32, 64 or 128 bits.
   No of Rounds = 1 to 255
   (Originally suggested 12 rounds)
5) It consists of a no. of modular additions and XORs.



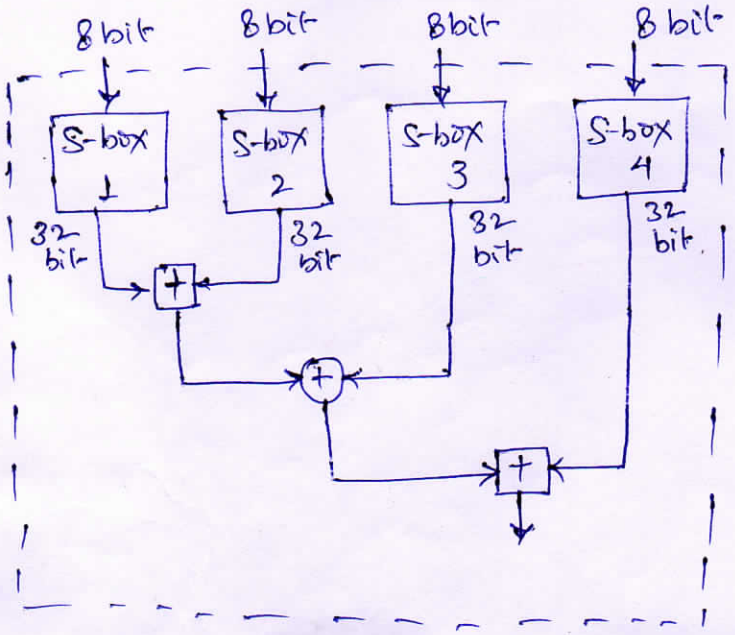
BLOWFISH CIPHER :-

1) It is a symmetric-key block cipher.
2). Designed in 1993 by Bruce Schneier.
3) It has a 64-bit block size and variable key length from 32 bits - 448 bits.
4.) It is a 16-round Feistel cipher.



Feistel Structure of Blowfish. (Each line represents 32 bits).

Round Function (F)



5). It keeps two subkey arrays : the 18-entry P-array and Four 256-entry S-box.
6) S-box accepts 8 bits input and produce 32-bit output.
7) One entry of the P-array is used every round. After the final round, each half of the data block is XORed with one of the two remaining unused P-entries.
8). Output of Round Function (F)
It is added modulo 2^{32} and XORed

Number Theory :-

Prime Number :- An integer that can only be divided without remainder by positive & negative values of itself and 1.

An integer $a > 1$ can be factored in a unique way as:

$$a = p_1^{a_1} p_2^{a_2} \ldots\ldots p_t^{a_t}$$

where: $p_1 < p_2 < \ldots\ldots < p_t$ are prime numbers and each a_i is a positive integer.

$$91 = 7 \times 13.$$
$$3600 = 2^4 \times 3^2 \times 5^2$$
$$11011 = 7 \times 11^2 \times 13.$$

If $\mathbf{P}$ is the set of all prime numbers, then any positive integer a can be written uniquely as:

$$a = \prod_{p \in P} p^{a_p}$$

where each $a_p \geq 0$.

Product over all possible prime numbers P.

Integer 12 is represented by $\{a_2 = 2, a_3 = 1\}$. $2^2 \cdot 3^1$

Integer 18 " " " $\{a_2 = 1, a_3 = 2\}$. $2^1 \cdot 3^2$

Integer 91 " " " $\{a_7 = 1, a_{13} = 1\}$. $7^1 \cdot 13^1$

FERMAT'S THEOREM :- If p is prime and a is a positive integer not divisible by p then we have

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{OR} \quad a^p \equiv a \pmod{p}$$

Example :-

(i) $a = 3, p = 5$

$3^{5-1} \equiv 3^4 \equiv 81 \equiv 1 \pmod 5$

$a = 3, p = 5$

$3^5 \equiv 3^5 \equiv 243 \equiv 3 \pmod 5$

(ii) $a = 4, p = 7$

$4^{7-1} \equiv 4^6 \equiv 1 \equiv 1 \pmod 5$

(iii) $a^9 = 7, p = 19$

$7^{19-1} \equiv 7^{18} \equiv 7^{16} \times 7^2$

$\equiv 7 \times 11$

$\equiv 1 \pmod{19}$.

$7^2 \equiv 49 \equiv 11 \pmod{19}$

$7^4 \equiv 121 \equiv 7 \pmod{19}$

$7^8 \equiv 49 \equiv 11 \pmod{19}$

$7^{16} \equiv 121 \equiv 7 \pmod{19}$

Euler's Totient function :- $\phi(n)$.

It is the no. of positive integers less than n and relatively prime to n.

Example:

① $\phi(37) = ?$

Becoz 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37.

So $\phi(37) = 36$

For a prime no. p
$\phi(p) = p-1$

② $\phi(35) = ?$

35 is not prime so we have to list all of the positive integers less than 35 that are relatively prime to it.

1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34.

$\phi(35) = 24$

Suppose we have two prime numbers p and q, with $p \neq q$, then we can show that for $n = pq$,

$$\phi(n) = \phi(pq) = \phi(p) \times \phi(q) = (p-1) \times (q-1)$$

Ex:- $\phi(21) = \phi(3) \times \phi(7) = 2 \times 6 = 12$.

1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20

Euler's Theorem :-

For every a and n that are relatively prime:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Example:

(i) $a = 3, n = 10$.

$\phi(10) = 4$. 1, 3, 7, 9

$a^4 = 3^4 \equiv 81 \equiv 1 \pmod{10}$

(ii) $a = 2, n = 11$

$\phi(11) = 10$.

$2^{10} = 1024 \equiv 1 \pmod{11}$

(iii) $a = 3, n = 7$.

$\phi(n) = \phi(7) = 6$.

$3^6 = 729 \equiv 1 \pmod{7}$

(iv) $a = 5, n = 9$.

$\phi(9) = 6$ 1, 2, 4, 5, 7, 8.

$a^6 = 5^6 = 15625 \equiv 1 \pmod{9}$

CHINESE REMAINDER THEOREM (CRT)

1) It is possible to reconstruct integers in a certain range from their residue modulo a set of pairwise relatively prime modulo.

2). If the prime factors of n are $p_1 * p_2 * p_3 * \dots p_t$, then the system of equation

$$x \bmod p_i = a_i \quad \text{where } i = 1, 2, \dots t.$$

has a unique solution x, provided $x < n$.

Example (1) $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

→ All 10 integers in Z_{10} can be reconstructed from their residue modulo 2 and 5 (relatively prime factors of 10).

→ The known residues of a decimal digit x are $r_2 = 0$ and $r_5 = 3$: that is $x \bmod 2 = 0$ and $x \bmod 5 = 3$

→ Therefore x is an even integer in Z_{10}. Unique Solution is $x = 8$.

Example (2) $Z_{35} = \{0, 1, 2, \dots \dots 33, 34\}$.

→ Relatively prime factors of $35 = 5$ and 7.

→ Residues of a decimal digit x are $r_5 = 1$, $r_7 = 2$.

→ Unique Solution is $x = 16$.

16 mod 5 | 16 mod 7.

Example (3) $x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$; $x \equiv 2 \pmod 7$.

Solve for x.

Answer :- For a decimal digit x, the residue class

$r_3 = 2$; $x_5 = 3$; $x_7 = 2$.

$x \bmod 3 = 2$ $\quad$ $x \bmod 5 = 3$ $\quad$ $x \bmod 7 = 2$

So the unique solution is $x = 23$

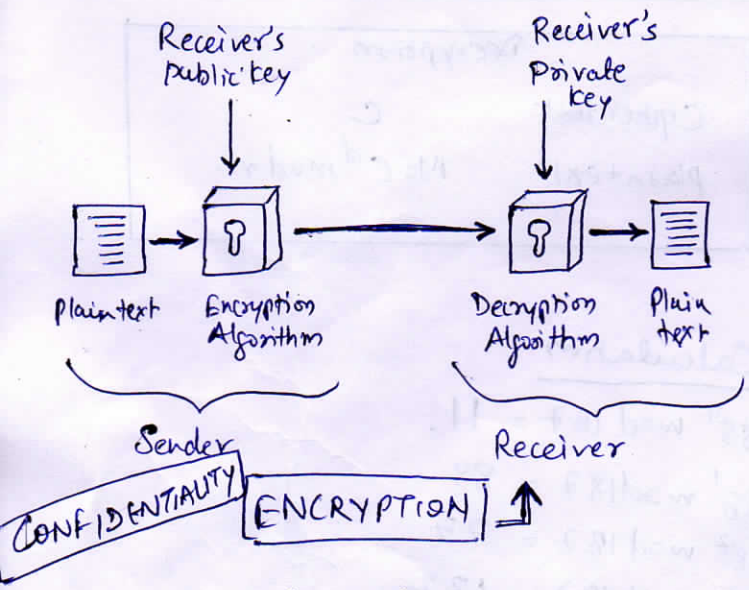
Issues with Symmetric Encryption:-

1) The ability to maitain total secrecy over communication.
2) Digital signatures.

Public key encryption (Asymmetric Encryption)

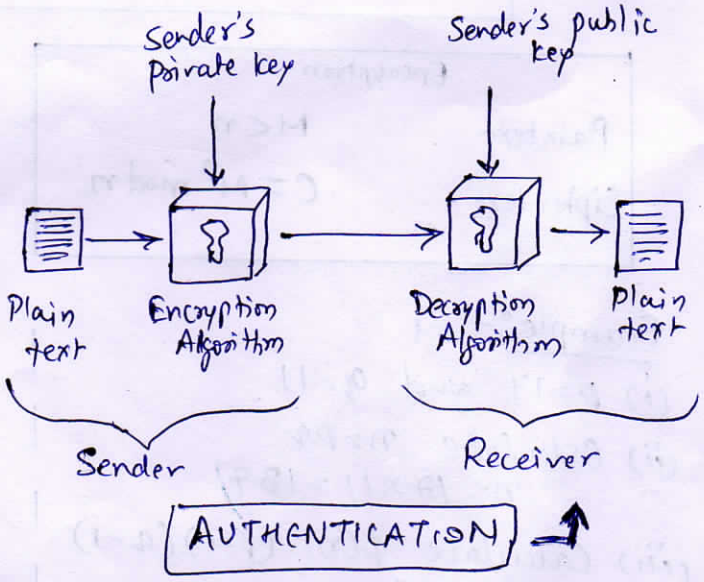
→ It is a form of crypto system in which encryption and decryption are performed using the different keys - one public key and one private key.

→ It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key.



$Y = E(PU_b, X)$

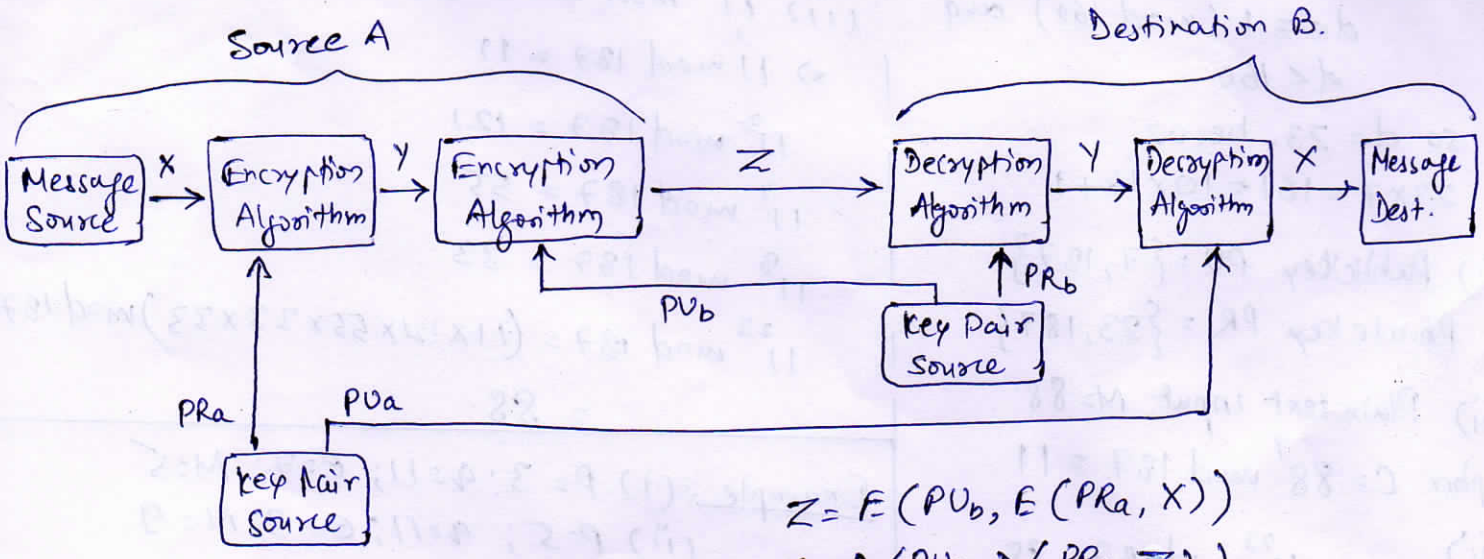
$X = D(PR_b, Y)$



$Y = E(PR_a, X)$

$X = D(PU_a, Y)$

AUTHENTICATION & SECRECY



$Z = E(PU_b, E(PR_a, X))$

$X = D(PU_a, D(PR_b, Z))$