Шифры:

1. Гаммирование -обязательно каждый четный или нечетный раунд. Длина гаммашифра = длина блока. Ключ = 16 байт.
2. Ключи – (процедура расширения ключа(можно но ненужно). Ключевой файл: [256 байт(sub); 16 байт(Gamma), 16 байт(Per), 8бит(Rol)]

Rol оператор (ключ 8 бит)

16 раундов:

1. Подстановка (ключ 256 байт)
2. Гаммирование (ключ 16 байт)
3. Перестановка (ключ 16 байт)
4. Гаммирование (ключ 16 байт)

И тд