1. Задание
2. Выполнение работы подразумевает создание параллельной программы для восстановления ключа симметричного шифрования DES (Data Encryption Standard) по известному открытому тексту методом полного перебора ключей(bruteforce).
3. Программа должна обеспечивать распределение подзадач по процессорам таким образом, чтобы обеспечить равномерную загрузку процессоров.
4. Для обмена сообщениями между процессорами использовать интерфейс передачи сообщений MPI(Message Passing Interface).
5. Описание

Множество *K* всех возможных ключей разбивается на непересекающиеся подмножества *K1, K2, … KN*. Система из *N* процессоров перебирает ключи так, что *i-*ый процессор осуществляет перебор ключей из множества *Ki, i=1..N*. Система прекращает работу, если один из процессоров нашёл ключ.

1. Алгоритм

* инициализация MPI и определение процессорной конфигурации

MPI\_Init(&argc, &argv);

MPI\_Comm\_size(MPI\_COMM\_WORLD,&numprocs);

MPI\_Comm\_rank(MPI\_COMM\_WORLD,&myid);

* 0-й процессор считывает шифр-текст и открытый текст из указанных параметрами файлов. Если параметры указаны неверно, выполнение прерывается.
* Рассылка считанных данных всем процессам

MPI\_Bcast(buf, buf\_size, MPI\_INT, 0, MPI\_COMM\_WORLD);

* Вычисление диапазана ключей для перебора.
* Перебор ключей ускоренным методом методом(bit\_slice). В случае обнаружения процессор выводит найденный ключ, происходит закрытие MPI и программа завершается:

MPI\_Abort(MPI\_COMM\_WORLD, 0);

exit(1);

* В противном случае, программа возвращает 0.