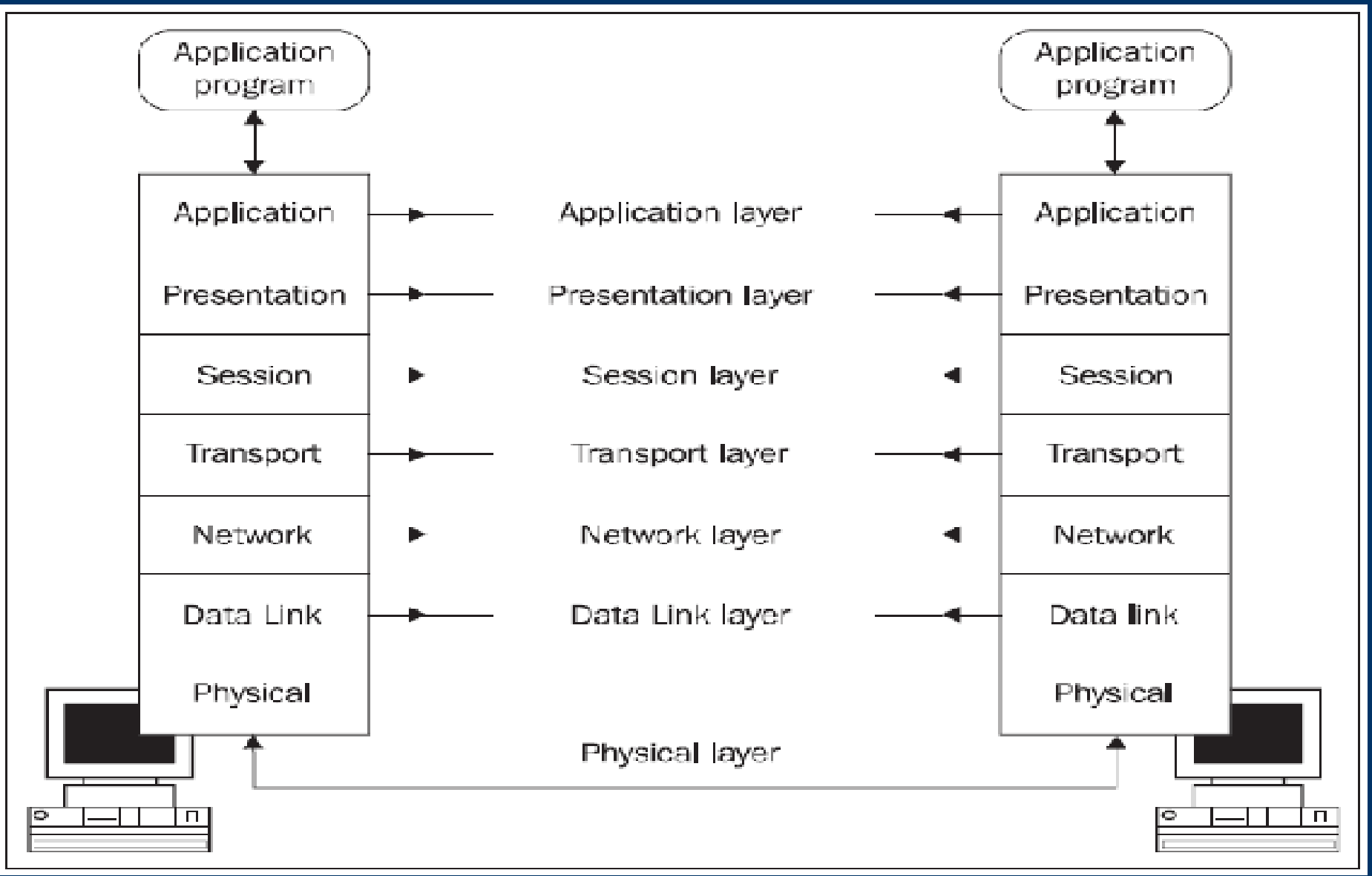
7-уровневая модель ISO/OSI

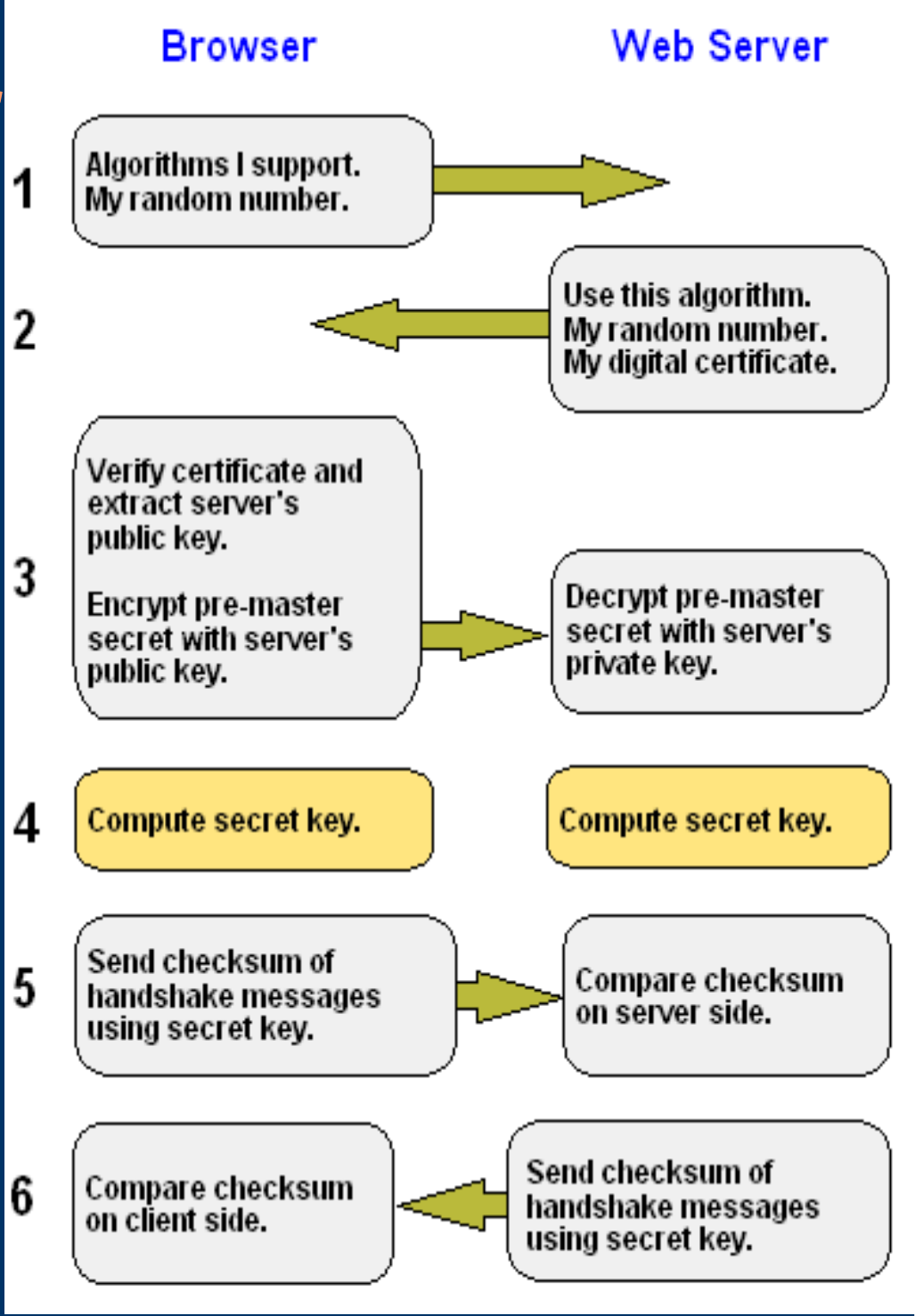


Уровень представления данных

- Форматы данных
- Шифрование
- Сжатие

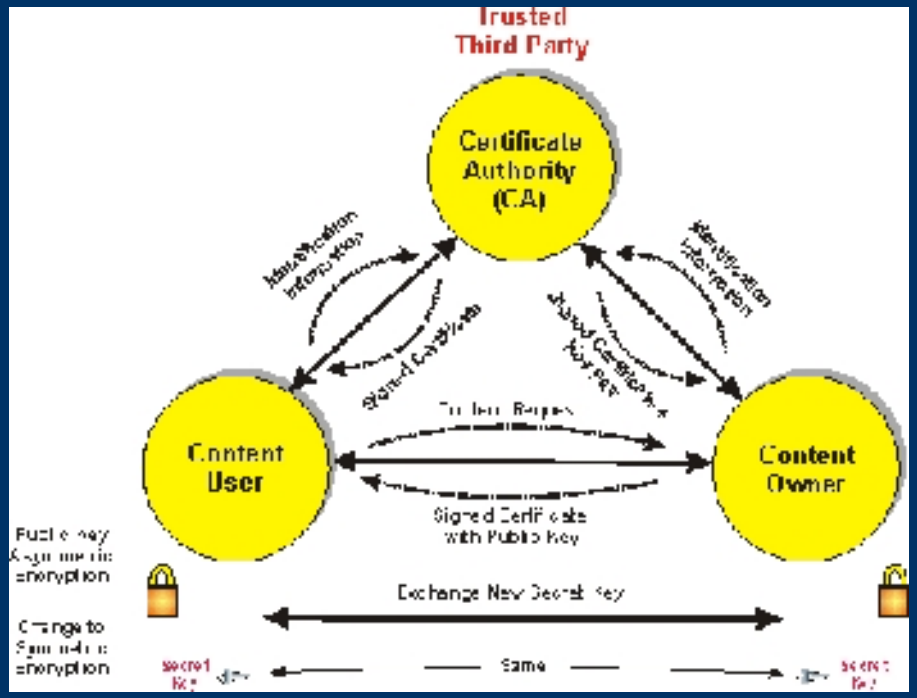
Secure Sockets Layer

- Асимметричное шифрование.
- Проверка подлинности сайта.
- Проверка целостности
- Интернет-банк, личная информация и т. д.



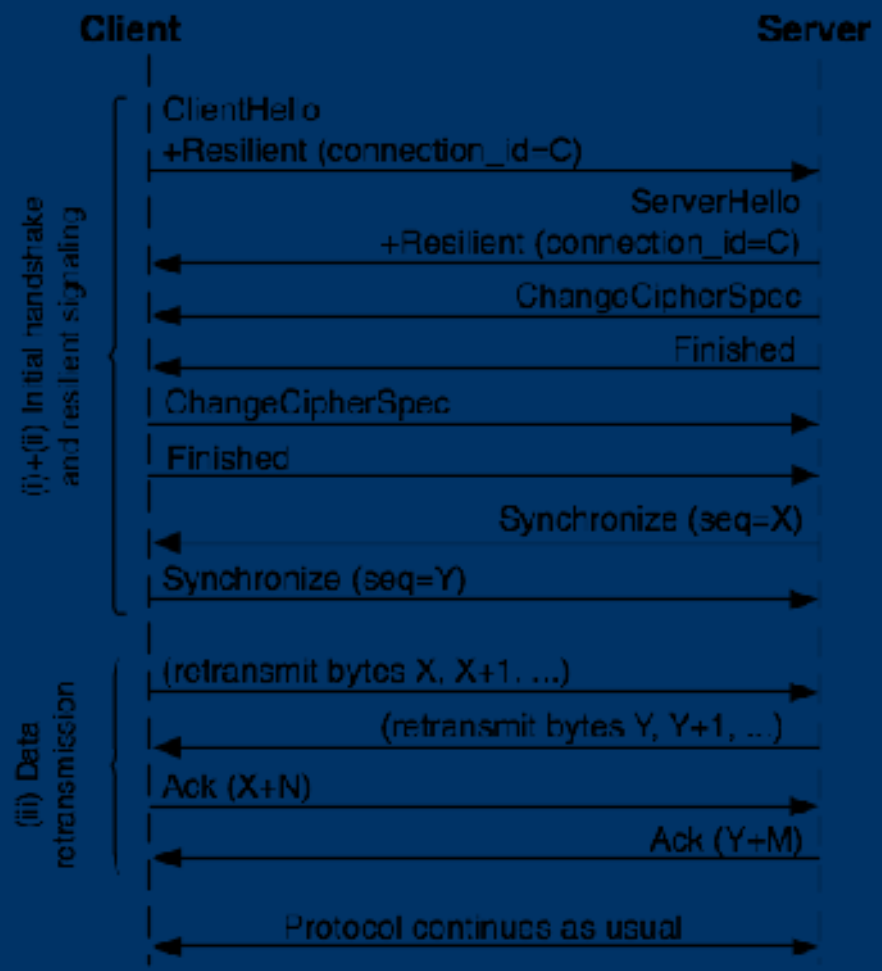
- Данные передаются в виде записей из заголовка и передаваемых данных. Заголовок содержит 2-3 байта кода длины, если старший бит в первом байте кода 1, то длина заголовка равна 2 байтам, иначе 3 байтам. Код длины записи не включает в себя число байт заголовка.
- Длина записи 2-байтового заголовка:
- RecLength = ((byte[0] & 0x7F) << 8) | byte[1];
- Длина записи 3-байтового заголовка:
- RecLength = ((byte[0] & 0x3F) << 8) | byte[1];
- Escape = (byte[0] & 0x40) != 0;
- Padding = byte[2];
- Padding определяет число байтов, добавленных, чтобы сделать длину записи кратной размеру блока шифра.
- Отправитель «заполненной» записи добавляет заполнитель и шифрует.
- Получатель записи дешифрует все поля данных и получает полную исходную информацию, заполнитель из поля данных удаляется.
- Данные записи SSL состоят из 3 компонент:
- MAC_Data[Mac_Size] — (Message Authentication Code) — код аутентификации сообщения Padding_Data[Padding] — данные заполнителя Actual_Data[N] — реальные данные
- Когда записи посылаются открытым текстом, длина Padding_Data и MAC_Data равны нулю. При использовании шифрования Padding_Data зависит от размера блока шифра, а MAC_Data зависит от выбора шифра. Пример вычисления MAC_Data:
- MacData = Hash(Secret, Actual_Data, Padding_Data, Sequence_Number);
- Здесь Sequence_Number представляет собой 32-битовый код, передаваемый хэш-функции в виде 4 байт, причём, первым передаётся старший байт. Для MD2, MD5 MAC_Size равен 16 байтам (128 битам). Для 2-байтового заголовка максимальная длина записи равна 32767 байтов, а для 3-байтного заголовка — 16383 байтов

Удостоверяющий центр



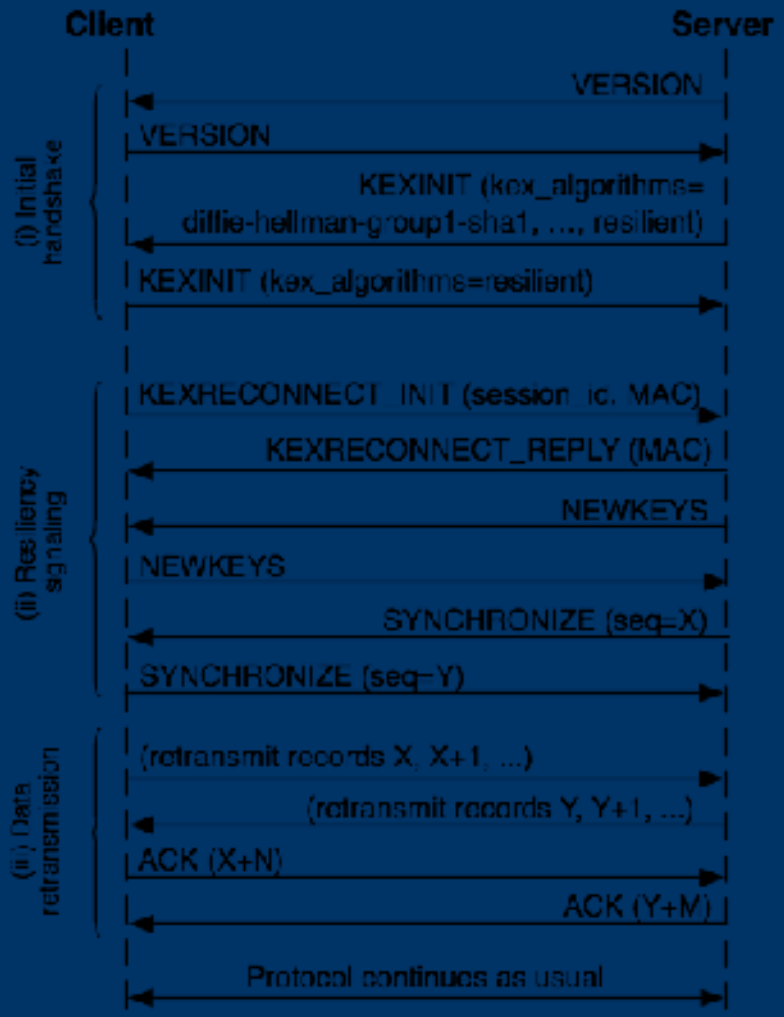
- Подтверждение подлинности
- Подчинение вышестоящему удостоверяющему центру
- Подчинение законодательству
- Платная услуга

Transport Layer Security



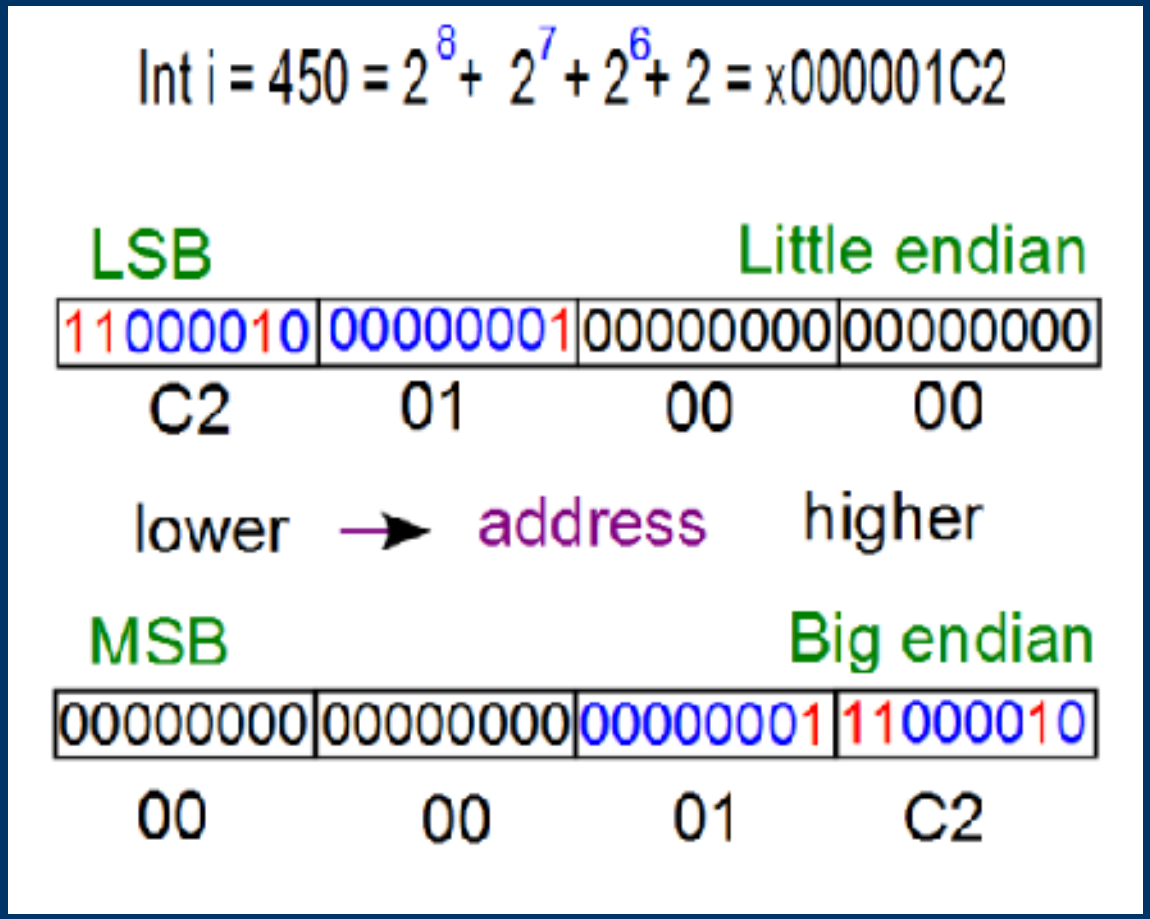
- Невидим для протоколов более высокого уровня
- Работает только на базе TCP

Secure SHell



- ssh -X -i private_key login@example.com

Порядок байтов



- htons(); htonl(); ntohs(); ntohl();

eXternal Data Representation

- boolean
- int (32-битное целое число)
- hyper (64-битное целое число)
- float
- double
- enumeration
- structure
- string
- массивы фиксированной длины
- массивы переменной длины
- неформатированные («сырые») данные

Кодировки

- UTF-8
- KOI-8
- CP-1251
- iconv -f KOI-8 -t UTF-8 file.koi8 > file.utf8

Графические форматы

- Jpeg, bmp, png — без движения
- GIF — с анимацией