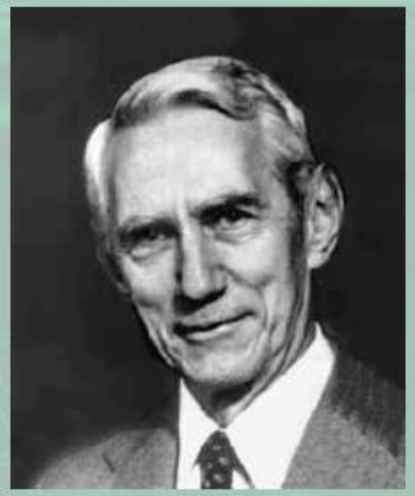
Совершенные шифры

Зубов А.Ю. Совершенные шифры. - М.: Гелиос АРВ, 2003. - 160 с., ил.

Потоковое шифрование

Большую популярность потоковым шифрам принесла работа **Клода Шеннона**, опубликованная в 1949 году, в которой Шеннон доказал абсолютную стойкость **шифра Вернама**(также известного, как одноразовый блокнот). В шифре Вернама ключ имеет длину, равную длине самого передаваемого сообщения. Ключ используется в качестве **гаммы**, и если каждый бит ключа выбирается случайно, то вскрыть шифр невозможно (т.к. все возможные открытые тексты будут равновероятны).



До настоящего времени было придумано немало алгоритмов потокового шифрования. Такие как: A3, A5, A8, RC4,PIKE, SEAL, eSTREAM.

http://rpp.nashaucheba.ru/pars_docs/refs/171/170122/img2.jpg

- **Шеннон** назвал *шифр совершенным*, если ни один шифртекст не раскрывает никаких сведений о соответствующем ему открытом тексте. Это означает, что для совершенных шифров апостериорные вероятности открытых текстов (вычисленные после получения криптограммы) совпадают с их априорными вероятностями.

- Шифр совершенный по К.Шеннону - это шифр с неограниченным ключом, и критерием совершенности для такого шифра является свойство совершенности составляющих его опорных шифров.
- Шифр с ограниченным ключом не является совершенным.