Лекция 5. Шифрование с открытым и закрытым ключом

1 Принципиальная схема шифрования

Шифрование с закрытым ключом: есть $Encoder(m, d)$, который передает сообщение c полиномиальной длины $Decoder(d, c) \to m$. Нужно чтобы перехватчик $A(c)$ не мог восстановить m.

Шифрование с открытым ключом: $Encoder(m, e)$ передает c программе $Decoder(c, d) \to m$. Ключи e, d у них разные, и перехватчик $A(c, d)$ может пользоваться одним из них.

Для закрытого ключа есть идеальная, но довольно бесполезная процедура: передать $m \oplus d$, где d — случайная строка. Есть две проблемы: ключ по длине равен сообщению (если мы можем обменяться такими ключами, то почему не можем обменяться сообщениями?), но даже если предположить, что мы заранее договорились о закрытом ключе, то остается проблема того, что шифр одноразовый: если известно $m_1 \oplus d$ и $m_2 \oplus d$, то можно узнать $m_1 \oplus m_2$, что может быть полезной информацией.