Криптографические рекомендации

Plain encryption	AEAD
Enc-and-MAC, MAC-then-Enc	Enc-then-Mac
Ассим. подпись	MAC
Откр./хэш. пароль	PBKDF2, bcrypt, scrypt
PRNG	KDF
Каскадный шифр	—
CBC	CTR
MD5, SHA1	RIPEMD, SHA3(?), Skein
SHA2-256	SHA2-512
PKCS N1 v1.5, plain RSA	PSS, OAEP
CBC, CMC, EME, LRW, XEX, MCB	XTS
GCM, EAX	OCB
PAP, CHAP, EKE	SRP
RC4	Salsa20

Не забывать при использовании PGP

- Расширять Web-of-Trust
- Для удобства и не потери WoT — использовать подключи
- Сразу же генерировать сертификат отзыва
- Хранить master-ключ в отдельном от подключей месте
- Обновлять подключи

Что делать с криптографическим ПО

- **Только** собственно сгенерированные ключи
- Шифровать ключи парольными фразами
- **Никогда** не забывать о качестве используемого PRNG: предоставлять достаточно энтропии, сохранять состояние (seed), постобработка для компрессии энтропии
- Предпочесть симметричную асимметричной криптографии
- Предпочесть RSA/ElGamal/DH основанным на эллиптических кривых алгоритмам
- Предпочесть darknet/F2F сети обычным opennet/P2P

Что делать с обыденным ПО

- **Только** открытое и/или свободное ПО
- **Только** известные открытые совместимые криптоалгоритмы, не изобретать своих
- Очищать cookie, логи, истории, кэши, временные файлы (диск в памяти?)
- Безопасно удалять с жёсткого диска файлы (шифрованный диск?)
- Не использовать одни и те же аутентификационные данные на разных сайтах, сервисах
- Забыть о паролях и использовать парольные фразы
- Использовать сертификаты и ключи вместо паролей
- Использовать сильные протоколы аутентификации
- Не забывать что email и IM не аутентифицирует собеседников
- Не забывать о PFS свойстве SSH, TLS (не всегда), OTR