# Хеш функции

Средство аутентификации

- M произвольной длины

- Н(M) фиксированной длины

- дешевизна вычисления

- необратимость (H(M)<-M)

- M1!=M2 -> H(M1)!=H(M2)

Message Digest (MD)

MD5

Birthday-коллизия

Secure Hash Algorithm (SHA)

SHA1

Данные 512

Хэш 160

SHA2

512/1024

256/224 **512**/384

SHA3

512/1024

256/224 **512**/384

Лавинный эффект (avalanche)

Конфузия и диффузия