gi

**SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.**

**SHA-3 Стандарт: Хеш-функции на основе перестановок и функции расширенного вывода (XOFs)**

**Аннотация**

Этот стандарт определяет семейство функций алгоритма безопасного хеширования (**Secure Hash Algorithm-3, SHA-3**) для двоичных данных. Каждая из функций SHA-3 основана на требованиях, установленных алгоритмом KECCAK, который Национальным институтом стандартов и технологий

США (**NIST – National Institute of Standards and Technology**) был выбран в качестве победителя конкурса **SHA-3 Cryptographic Hash Algorithm**. Это стандарт также определяет семейство математических перестановок **KECCAK-p**, включающих перестановку, лежащую в основе **KECCAK**, для облегчения разработки дополнительных криптографических функций на основе перестановок.

Семейство SHA-3 состоит за четырёх криптографических хеш-функций: SHA3-224, SHA3-256, SHA3-384 и SHA3-512; и двух функций расширенного вывода (**XOFs**): SHAKE128 и SHAKE256.

Хеш-функции являются компонентами многих важных приложений информационной безопасности, в частности: 1) генерация и верификация цифровых подписей; 2) формирование ключа; 3) генерация псевдослучайных битов. Хеш-функции, определенные в данном стандарте, дополняют хеш-функцию SHA-1 и семейство хеш-функций SHA-2, определенных в стандарте **FIPS (Federal Information Processing Standards) 180-4, the Secure Hash Standard**.

Функции расширенного вывода отличаются от хеш-функций, но их можно использовать аналогичным образом и гибко адаптировать непосредственно к требованиям конкретных приложений с учетом дополнительных соображений безопасности.

**1. Наименование стандарта:** Стандарт SHA-3: Хеш-функции, основанные на перестановках, и функции расширенного вывода (**FIPS PUB 202**).

**2. Категория стандарта:** Стандарт компьютерной безопасности, криптография.

**3. Объяснение:** …

Данные на входе хеш-функций называются **сообщением** (**message**), a на выходе – **дайджестом** (**digest**) или «хешем» (**hash value**). Сообщение может иметь различную длину, длина дайджеста **фиксирована**. Криптографическая хэш-функция – это хэш-функция, которая предназначена для обеспечения специальных свойств, включающих сопротивление коллизиям (**collision resistance**) и сопротивление прообразу (**preimage resistance**), которые важны для многих приложений в области информационной безопасности.