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:** Этот стандарт (FIPS 202) определяет семейство функций алгоритма криптографического хеширования (SHA-3) для двоичных данных. Каждая из функций SHA-3 базируется на принципах алгоритма KECCAK, который NIST выбрало в качестве победителя конкурса SHA-3 Cryptographic Hash Algorithm Competition. Это стандарт также определяет семейство математических перестановок KECCAK-p, включающих перестановку, лежащую в основе KECCAK. Указанные перестановки могут служить основными компонентами дополнительных криптографических функций, которые могут быть определены в будущем.

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

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 обладает специальными свойствами, включающими в себя сопротивление коллизиям (**collision resistance**) и сопротивление прообразу (**preimage resistance**), которые важны для многих приложений в области информационной безопасности. К примеру, криптографическая хеш-функция увеличивает безопасность и эффективность схемы цифровой подписи в том случае, когда вместо сообщения цифровой подписью подписывается дайджест. В этом контексте сопротивление хеш-функции коллизиям обеспечивает уверенность в том, что оригинальное сообщение не могло быть изменено на другое сообщение с тем же значением хеш-функции и, следовательно, с той же подписью. Другое приложение криптографических хеш-функций включает в себя генерацию псевдослучайных чисел (**pseudorandom bit generation**), имитовставки (**message authentication codes**) и функции формирования ключа (**key derivation functions**).

Четыре хеш-функции SHA-3, определенные в этом стандарте, дополняют хеш-функции, которые определены в FIPS 180-4: семейство SHA-1 и SHA-2. Оба стандарта вместе обеспечивают устойчивость к будущим достижениям в области криптоанализа хеш-функций, поскольку они основаны на принципиально разных принципах проектирования. Помимо разнообразия дизайна, хеш-функции в данном стандарте обеспечивают некоторые дополнительную реализацию и характеристики производительности по сравнению с FIPS 180-4.

Длина выходных данных для XOFs может быть выбрана под требования конкретного приложения. Сами функции расширенного вывода могут быть адаптированы для хеш-функций в связи с дополнительными соображениями безопасности, или использованы во множестве других приложений. Соответствующее использование XOFs будет определено в специальных публикациях NIST.

Перестановки KECCAC-p были разработаны для использования в качестве главных компонентов для множества криптографических функций, включая ключевые функции для аутентификации и/или шифрования (**keyed function for authentication and/or encryption**). Шесть функций SHA-3 могут быть рассмотрены в качестве модов (**modes**) операции перестановки **KECCAC-p[1600, 24]**. В будущем дополнительные моды этой перестановки или другие перестановки KECCAC-pа могут быть определены и одобрены в публикациях FIPS или специальных публикация NIST (**NIST Special Publications**).

**4. Право одобрения (Approving Authority):** Министр торговли (Secretary of Commerce).

**5. Подразделение поддержки (Maintenance Agency):** Департамент торговли США (U.S. Department of Commerce), Национальный институт стандартов и технологий (NIST), Лаборатория информационной технологии (**Information Technology Laboratory, ITL**).

**6. Применимость (Applicability):** Данный стандарт применим для всех федеральных департаментов и агенств (Federal departments and agencies)