

УДК 681.3.06

Принцип построения «инволютивных» шифров / С.А. Головашич // Проблемы бионики. Всеукр. межвед. науч.-техн. сб. 2001. Вып. 000. С. 00—00.

Предложен общий принцип построения блочных симметричных шифров с идентичными процедурами прямого и обратного преобразований. Конструкции данного класса позволяют существенно сократить затраты на реализацию шифратора. Приведены примеры цикловых преобразований на основе Фейстель-подобной и IDEA-подобной цепи.

Табл. 0. Ил. 3. Библиогр.: 3 назв.

УДК 681.3.06

Принцип побудови «інволютивних» шифрів / С.О. Головашич // Проблеми біоніки. Всеукр. міжвід. наук.-техн. зб. 2001. Вип. 000. С. 00—00.

Запропоновано загальний принцип побудови блокових симетричних шифрів з ідентичними процедурами прямого та зворотного перетворень. Конструкції даного класу дозволяють істотно скоротити затрати на реалізацію шифратора. Наведено приклади циклових перетворень на основі Фейстель-подібного та IDEA-подібного цепу.

Табл. 0. Іл. 3. Бібліогр.: 3 назви.

UDC 681.3.06

The design principle of «involution» ciphers / S.A. Golovashich // Problems of bionics. All-Ukr. Sci. Interdep. Mag. 2001. N 000. P. 00—00.

The general principle of symmetric block cipher design with identical encryption and decryption transformation is proposed. Using that kind of structure allows significantly to reduce outlay on cipher implementation. Examples of round transformations based on Feistel-like and IDEA-like networks are given.

0 tab. 3 fig. Ref.: 3 items.