ВСТУП

На даний момент у світі надзвичайно активно використовуються інформаційні технології, в першу чергу ті, що пов’язані з обміном інформацією. Це зумовлює необхідність забезпечувати захищену передачу даних, як персональних, так і пов’язаних з комерцією або державною таємницею. Жодний віддалений спосіб комунікації не може бути надійно захищений без криптографічних засобів захисту інформації. Криптографічні примітиви є сукупністю певних алгебраїчних перетворень і властивості їх можна використати для захисту від порушення конфіденційності та цілісності інформації. Загальновідомим є факт про комплементарність шифру DES. Ця властивість зменшує ефективну довжину ключа на один біт. Розвинувши теорію щодо властивостей комплементарності інших схем шифрування, можна будувати ефективні атаки на них. Проте, інтенсивні дослідження в цьому напрямку проводили тільки А. Бірюков та І. Ніколіч [1]. Вони дослідили комплементарність фейстелівських схем шифрування та розробили атаки на режим гешування для алгоритму Camellia-128 та шифр ГОСТ 28147-89. Отримані ними результати можна проінтерпретувати для інших фейстель-подібних схем шифрування.