В чому основне призначення ФГ в криптографічних додатках? Які ФГ можуть бути застосовані в Україні?

Геш-функції в основному призначені для ідентифікації повідомлень довільної бітової довжини. Також, геш-фунцкії можна використовувати для генерації псевдовипадкових ключів та перевірки цілісності повідомлень. В Україні можна користуватися наступними геш-функціями:

1) SHA-3 «Keccak»
2) ДСТУ 7564:2014
3) ДСТУ ГОСТ 34.311:2009
4) SHA-2