Exemplu de subiect pentru examen

1. Atacuri asupra securitatii informatiei. Clasificarea atacurilor *
2. Criptarea AES. Functiile SubBytes( ), ShiftRows( ), MixColumns( ), AddRoundKey( )
3. a. Ce este criptologia?
   b. Generarea subcheilor in algoritmul IDEA (numai subcheile pentru criptare).
   c. Autoritate pentru distibutia cheilor publice.