crypto 1014

Quiz for week 3

姓名

1. Winning a lottery with 1 million contestants ??? (the biggest number) times in a row is easier than correctly guessing a random 256-bit AES key on the first try. ??? =

2. Suppose that using commodity hardware it is possible to build a computer for about $2000 that can brute force about 1 trillion AES keys per second. Suppose an organization wants to run an exhaustive search for a single 128-bit AES key and was willing to spend 4 trillion dollars to buy these machines (this is more than the annual US federal budget, for 2016, US federal budget is $3.999 trillion). How many years would it take the organization to brute force this single 128-bit AES key with these machines? (Ignore additional costs such as power and maintenance. Use billion to evaluate with 1 digit after the decimal point,such as 8.7 means 8.7 billion years.

3. Let F be a secure pseudorandom function with 128-bit key and 256-bit block length. Which are the following functions G are secure pseudorandom generators? (Select all that apply.) 【多选题】

- A、G(x)=Fx(0...0), where x is a 128-bit input.
- B、G(x)=Fx(0...0)‖Fx(0...0), where x is a 128-bit input.
- C、G(x)=Fx(0...0)‖Fx(1...1), where x is a 128-bit input.
- D、G(x)=F0...0(x)‖F1...1(x), where x is a 256-bit input

4. Say we use CBC-mode encryption based on a block cipher with 256-bit key length and 128-bit block length to encrypt a 512-bit message. How long is the resulting ciphertext?

5. Let m be a message consisting of ℓ AES blocks (say ℓ=100). Alice encrypts m using CBC mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number ℓ/2 is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly. Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted?

6. Let m be a message consisting of ℓ AES blocks (say ℓ=100). Alice encrypts m using randomized counter mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number ℓ/2 is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly. Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted?

提交