

**Facultat d'Informàtica de Barcelona**  
**Examen final de Criptografia**  
**21 de juny de 2010**

1. Els xifratges de Cèsar, Vigenère i Vernam són xifratges de \_\_\_\_\_. La funció de xifratge es pot expressar amb una mateixa fórmula per a tots tres: \_\_\_\_\_. Explica el significat de la fórmula en cada cas.
  
2. Què té el xifrat de Vernam que el diferencia de qualsevol altre mètode de xifratge?
  
3. L'algoritme AES fa operacions al cos finit \_\_\_\_\_. Un generador del grup multiplicatiu d'aquest cos és \_\_\_\_\_. La darrera volta de l'algoritme es diferencia de les anteriors en que \_\_\_\_\_.
  
4. Suposem que una seqüència de blocs de text  $m_1, \dots, m_n$  es xifra usant un xifratge de bloc i un mode d'operació. Suposem també que un bloc de criptograma, diguem-ne  $c_i$ , es transmet incorrectament. Quins blocs de missatge es desxifraràn incorrectament si el mode d'operació és ECB? I si s'utilitza el mode CBC? Justifica la resposta.
  
5. El test de primalitat més utilitzat en Criptografia és el test de \_\_\_\_\_. En quines propietats dels nombres primers es basa?
  
6. Cita tres algorismes criptogràfics que requereixen generació eficient de nombres primers de longitud fixada. Descric breument el paper del nombre primer en cadascun d'ells.

7. Explica com s'utilitza el *Teorema Xinès de les Restes* per accelerar el desxifrat RSA.
8. Suposem que  $n$  és una clau RSA. Prova que conèixer el valor de  $\varphi(n)$  és computacionalment equivalent a factoritzar  $n$ .
9. El millor algoritme de factorització conegut té complexitat \_\_\_\_\_. Amb ell, el rècord de factorització s'ha situat recentment en claus RSA de \_\_\_\_\_ bits. Per això, el tamany mínim d'una clau RSA emesa actualment és de \_\_\_\_\_ bits.
10. Per generar aleatòriament un punt d'una corba el·líptica  $E/\mathbb{F}_p : y^2 = x^3 + ax + b$  fem el següent: triem una abscissa  $x \in \mathbb{F}_p$  \_\_\_\_\_, calculem \_\_\_\_\_, després calculem \_\_\_\_\_ usant l'algoritme \_\_\_\_\_. Si obtenim \_\_\_\_\_, triem una nova  $x$  i repetim el procés. Si obtenim \_\_\_\_\_, sabem que \_\_\_\_\_ és un \_\_\_\_\_ de  $\mathbb{F}_p$  i calculem l'ordenada  $y$ , que és una \_\_\_\_\_. Si  $p \equiv 3 \pmod{4}$ , aleshores  $y$  es pot calcular fent \_\_\_\_\_.
11. Cita les propietats més importants d'una funció hash.

L'algoritme MD5 es considera trencat perquè \_\_\_\_\_.

L'algoritme SHA-1 es considera trencat perquè \_\_\_\_\_.

12. Un certificat digital és un document \_\_\_\_\_ per una \_\_\_\_\_ que estableix \_\_\_\_\_.

El format estàndard dels certificats digitals és el \_\_\_\_\_. Una autoritat certificadora arrel és \_\_\_\_\_.

En els cas del DN i l'autoritat certificadora arrel usa claus \_\_\_\_\_ de \_\_\_\_\_ bits.

**Cada pregunta 0.5 punts**

**Les notes es publicaran al Racó el dia 25 de juny**

**La revisió (de l'examen i les pràctiques) serà el dia 28, a las 10h. al despatx 338 de l'edifici Omega**

**Facultat d'Informàtica de Barcelona**  
**Cryptography final**  
**June 21st., 2010**

1. Caesar, Vigenère and Vernam cryptosystems are \_\_\_\_\_ cryptosystems. The enciphering function can be expressed using the same formula for the three of them: \_\_\_\_\_. Explain the meaning of the formula in each case.
  
2. What makes Vernam cipher different from any other cryptosystem?
  
3. AES algorithm performs operations on the finite field \_\_\_\_\_. A generator for its multiplicative group is \_\_\_\_\_. Last round of the algorithm is different from the others because \_\_\_\_\_.
  
4. Suppose that a sequence of plaintext blocks  $m_1, \dots, m_n$  is encrypted using a block cipher and an operation mode. Suppose also that one ciphertext block, say  $c_i$ , is transmitted incorrectly. Which plaintext blocks will be decrypted incorrectly if the operation mode is ECB? And if the operation mode is CBC? Justify the answer.
  
5. The primality test most commonly used in Cryptography is \_\_\_\_\_ test. On which properties of prime numbers is it based?
  
6. Name three cryptographic algorithms which require efficient generation of prime numbers of a given length. Give a brief description of the role of the prime number in each of them.

7. Explain how the *Chinese Remainder Theorem* is used to speed up RSA decryption.
8. Assume that  $n$  is an RSA key. Show that the knowledge of  $\varphi(n)$  is computationally equivalent to the factorization of  $n$ .
9. The best known factorization algorithm has \_\_\_\_\_ complexity. Using it, the factorization record has recently reached RSA keys of \_\_\_\_\_ bits. Because of that, a key length of \_\_\_\_\_ bits is considered the minimum necessary for the RSA encryption algorithm.
10. In order to generate a random point of an elliptic curve  $E/\mathbb{F}_p : y^2 = x^3 + ax + b$  we follow these steps: choose an abscissa  $x \in \mathbb{F}_p$  \_\_\_\_\_, compute \_\_\_\_\_, then compute \_\_\_\_\_ using \_\_\_\_\_ algorithm. If we obtain \_\_\_\_\_, we choose a new  $x$  and repeat the procedure. If we obtain \_\_\_\_\_, we know that \_\_\_\_\_ is an \_\_\_\_\_ in  $\mathbb{F}_p$  and we compute the ordinate  $y$ , which is an \_\_\_\_\_. If  $p \equiv 3 \pmod{4}$ , then  $y$  can be computed as \_\_\_\_\_.
11. Name the most important properties of a hash function.

MD5 algorithm is considered broken because \_\_\_\_\_.

SHA-1 algorithm is considered broken because \_\_\_\_\_.

12. A digital certificate is a document \_\_\_\_\_ by \_\_\_\_\_ which establishes \_\_\_\_\_.

The standard format for digital certificates is \_\_\_\_\_. A root certificate authority is \_\_\_\_\_.

In case of Spanish DNIe the root authority uses \_\_\_\_\_ keys of \_\_\_\_\_ bitlength.

**Each question 0.5 points**

**Grades will be published at the Racó on June 25th.**

**Revision (of examen and labs) will be on June 28th. at 10h., office 338 of Omega building**