

NOM:

Facultat d'Informàtica de Barcelona
Criptografia
6 de juny de 2011

1. Quina de les següents afirmacions sobre DES és falsa?

- Les claus i els blocs són de 56 bits
- Es va trencar usant la cerca exhaustiva de claus
- Els detalls complets dels criteris de disseny de les caixes S no s'han fet públics
- Cap de les anteriors (és a dir, totes les afirmacions anteriors són certes)

2. Quina de les següents afirmacions sobre l'AES és certa?

- La clau ha de ser de 128 bits de longitud
- La NSA el va aprovar perquè els dissenyadors eren americans
- És un xifrat de bloc que es pot usar en mode CBC
- Cap de les anteriors (és a dir, totes les afirmacions anteriors són falses)

3. L'algoritme AES utilitza polinomis binaris mod $m(x) = x^8 + x^4 + x^3 + x + 1$ per representar $GF(2^8)$.
Quin és l'invers multiplicatiu de $0x0b = x^3 + x + 1$?

- 0x30 0x60 0xc0 Cap dels anteriors

4. Quina de les transformacions següents s'usa també en l'expansió de clau de l'AES?

- ByteSub ShiftRow MixColumn Cap de les anteriors

5. Per xifrar una sèrie de blocs de text m_1, m_2, \dots, m_k utilitzant un xifratge de bloc E operant en mode *Electronic Code Book* (ECB), els blocs de criptograma c_1, c_2, \dots, c_k es calculen fent $c_i = E_k(m_i)$. Quina de les següents **no** és una propietat d'aquest mode d'operació?

- Els blocs repetits donaran lloc a blocs de criptograma idèntics
- El desxifratge pot ser paral·lelitzat completament
- Si un bloc c_i de criptograma es modifica, accidentalment o voluntàriament, en el desxifratge resultarà afectat únicament el bloc m_i de missatge
- Cap de les anteriors (és a dir, totes les anteriors són propietats del mode ECB)

6.

Un espai de claus gran és suficient per garantir la seguretat d'un sistema criptogràfic

Cert Fals

Un bon algoritme de xifratge ha d'amagar les propietats estadístiques del missatge

Actualment, el límit de la capacitat computacional es situa al voltant de les 2^{80} operacions

No hi ha cap sistema criptogràfic que compleixi les condicions de secret perfecte de Shannon

El DES es considera trencat perquè no té bones propietats de confusió i difusió

Triple-DES és un estàndard encara vigent, amb 112 bits de longitud de clau

Els sistemes de xifratge en flux utilitzen generadors de nombres pseudoaleatoris

Els modes d'operació es poden fer servir amb xifratges de flux o de bloc indistintament

Si us plau, gira el full. L'examen segueix al revers.

7. Hem de calcular $x^{4760} \bmod n$ i $285P$, on P és un punt d'una corba el·líptica.
- El primer càlcul es pot fer amb un algoritme de complexitat polinòmica però el segon no.
 - El primer càlcul el podem fer amb menys de 26 productes mòdul n i el segon amb menys de 18 sumes a $E(\mathbb{F}_p)$.
 - El primer càlcul el podem fer amb menys de 26 operacions elementals i el segon amb menys de 18 operacions elementals.
 - Cap de les afirmacions anteriors és correcta.
8. En un sistema Diffie-Hellman, els paràmetres comuns són $p = 269$ i $x = 2$ i un parell d'usuaris tenen claus privades $a = 19$ i $b = 50$.
- Les claus públiques respectives són 7 i 30. La clau comuna és 108
 - Les claus públiques respectives són 37 i 10. La clau comuna és 108
 - Les claus públiques respectives són 7 i 30. La clau comuna és 208
 - Cap de les afirmacions anteriors és correcta.
9. Considerem la corba el·líptica E sobre \mathbb{F}_{23} definida per l'equació $y^2 = x^3 + 4x + 20$.
- La corba té un punt d'abscissa 7.
 - La corba té 41 punts diferents.
 - Si ens diuen que la corba té 41 punts, sabem que tots ells són múltiples de $P = (8, 10)$.
 - Totes les afirmacions anteriors són correctes.
10. En un certificat digital
- Figuren les claus públiques del propietari i de l'Autoritat Certificadora.
 - Figuren les claus pública i privada del propietari.
 - Figura la clau pública del propietari i la signatura digital de l'Autoritat Certificadora.
 - Totes les afirmacions anteriors són correctes
11. Una Autoritat Certificadora arrel
- sempre té Autoritats Certificadores subordinades
 - és una Autoritat Certificadora que es certifica a sí mateixa
 - té claus pública i privada amb un període de validesa més curt que el dels certificats que emet
 - Totes les afirmacions anteriors són correctes
12. El DNI elèctronic
- Conté certificats de ciutadà amb claus RSA de 2048 bits.
 - Conté certificats X.509 v3 i claus Diffie-Hellman.
 - Té una jerarquia de certificació amb una autoritat arrel i una subordinada que emet els certificats de ciutadà.
 - Totes les afirmacions anteriors són correctes.

Resposta correcta = + 1/2 Resposta incorrecta = - 1/6 No resposta = 0

Notes: dia 14 de juny

Revisió (examen i pràctiques): dia 15 de juny a les 10h. Despatx 338 Edifici Omega

NAME:

Facultat d'Informàtica de Barcelona
Criptografia
June 6th, 2011

1. Which statement about DES is false?

- The underlying cipher was broken using exhaustive search
- The keys and blocks are 56 bits in length
- The full design criteria for the S-Box design is not public
- None of the above (that is, all the above statements are true)

2. Which of the following is true about AES?

- The keys must be 128 bits long
- The NSA approved it because the developers were American
- It is a block cipher that can be used in CBC mode
- None of the above (that is, all the above statements are false)

3. AES algorithm uses binary polynomials mod $m(x) = x^8 + x^4 + x^3 + x + 1$ to represent $GF(2^8)$. Which one is the multiplicative inverse of $0x0b = x^3 + x + 1$?

- 0x30 0x60 0xc0 None of the above

4. Which of the following transformations is also used in AES key expansion?

- ByteSub ShiftRow MixColumn None of the above

5. To encrypt a series of plaintext blocks m_1, m_2, \dots, m_k using a block cipher E operating in electronic code book (ECB) mode, each ciphertext block c_1, c_2, \dots, c_k is computed as $c_i = E_k(m_i)$. Which of the following is **not** a property of this block cipher mode?

- Any repeated plaintext blocks will result in identical corresponding ciphertext blocks.
- Decryption can be fully parallelized.
- If a ciphertext block c_i is modified or corrupted, then after decryption only the corresponding plaintext block m_i will be affected.
- None of the above (that is, all the above are properties of the ECB block cipher mode).

6.

	True	False
A large key space is enough to guarantee a strong encryption system	<input type="checkbox"/>	<input type="checkbox"/>
A good cipher should hide the statistical properties of plaintext	<input type="checkbox"/>	<input type="checkbox"/>
Currently, the safety limit for computational capacity is estimated in 2^{80} operations	<input type="checkbox"/>	<input type="checkbox"/>
There isn't any cryptographic system that satisfies Shannon's perfect secret conditions	<input type="checkbox"/>	<input type="checkbox"/>
DES is considered broken because it does not have good confusion and diffusion properties	<input type="checkbox"/>	<input type="checkbox"/>
Triple-DES is a current standard, with 112 bit key length	<input type="checkbox"/>	<input type="checkbox"/>
Stream ciphers use pseudorandom number generators	<input type="checkbox"/>	<input type="checkbox"/>
Operation modes can be used with both stream ciphers and block ciphers	<input type="checkbox"/>	<input type="checkbox"/>

Please turn this page over and continue with questions on the reverse.

7. We have to compute $x^{4760} \bmod n$ and $285P$, with P a point on an elliptic curve.
- First computation can be done with less than 26 elementary operations and the second one with 18 elementary operations.
 - First computation can be done with less than 26 products mod n and the second one with less than 18 additions in $E(\mathbb{F}_p)$.
 - First computation can be done with an algorithm of polynomial complexity, but the second one can not.
 - None of the above statements is correct.
8. In a Diffie-Hellman system, common parameters are $p = 269$ and $x = 2$, and a pair of users have private keys $a = 19$ and $b = 50$.
- Respective public keys are 7 and 30. Common key is 108.
 - Respective public keys are 7 and 30. Common key is 208.
 - Respective public keys are 37 and 10. Common key is 108.
 - None of the above statements is correct.
9. Let us consider the elliptic curve E over \mathbb{F}_{23} defined by equation $y^2 = x^3 + 4x + 20$.
- There is a point with abscissa 7.
 - The curve has 41 different points.
 - If we are told that the curve has 41 points, then we know that all of them are multiples of $P = (8, 10)$.
 - All of the above statements are correct.
10. In a digital certificate
- one can find the public keys of the owner and the Certificate Authority.
 - one can find the public and private keys of the owner.
 - one can find the public key of the owner and the digital signature of the Certificate Authority.
 - All the above statements are correct.
11. A root Certificate Authority
- has always subordinate Certificate Authorities.
 - is a Certificate Authority which issues self-signed certificates.
 - has public and private keys with shorter validity periods than the certificates it issues.
 - All the above statements are correct.
12. Spanish electronic Identity Card
- contains citizen certificates with RSA keys of 2048 bits.
 - has a certification tree with a root authority and a subordinate authority. The last one issues the citizen certificates.
 - contains certificates X.509 v3 and Diffie-Hellman keys.
 - All the above statements are correct.

Right answer = + 1/2 Wrong answer = - 1/6 No answer = 0

Grades: June, 14th.

Revision (exam and labs): June, 15th. at 10h. Office 338 Omega building