

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 1
- (a) Encryption / le chiffrement
  - (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 0
- (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 2
- (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - (c) substitutions / des substitutions
  - (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 2
- (a) often improves usability / améliore souvent l'utilisabilité
  - (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 0
- (a) Encryption / le chiffrement
  - (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - ☒ (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

### Question 2 (2 points)

Digital signature : / La signature numérique :

- 1
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - (d) may use hash functions / peut utiliser des fonctions de hachage

signature → certificat → authentification

### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 3
- (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - ☒ (c) substitutions / des substitutions
  - ☒ (d) transpositions / des transpositions

### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

### Question 5 (2 points)

Security: / La sécurité:

- 2
- (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Écrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- ☒ (a) Encryption / le chiffrement
- ☐ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
- ☒ (c) Digital signature / la signature numérique
- ☐ (d) Hash functions / les fonctions de hachage

### Question 2 (2 points)

Digital signature : / La signature numérique :

- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
- ☐ (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
- ☐ (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
- ☐ (d) may use hash functions / peut utiliser des fonctions de hachage

### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- ☒ (a) permutations / des permutations
- ☐ (b) corruptions / des corruptions
- ☒ (c) substitutions / des substitutions
- ☐ (d) transpositions / des transpositions

### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- ☒ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
- ☐ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
- ☐ (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
- ☐ (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

### Question 5 (2 points)

Security: / La sécurité:

- ☐ (a) often improves usability / améliore souvent l'utilisabilité
- ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
- ☐ (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
- ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 1
- ☒ (a) Encryption / le chiffrement
  - ☐ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - ☐ (c) Digital signature / la signature numérique
  - ☐ (d) Hash functions / les fonctions de hachage

### Question 2 (2 points)

Digital signature : / La signature numérique :

- 1
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - ☐ (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - ☐ (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - ☐ (d) may use hash functions / peut utiliser des fonctions de hachage

### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 0
- ☐ (a) permutations / des permutations
  - ☐ (b) corruptions / des corruptions
  - ☒ (c) substitutions / des substitutions
  - ☐ (d) transpositions / des transpositions

### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 1
- ☒ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - ☐ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - ☐ (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - ☐ (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

### Question 5 (2 points)

Security: / La sécurité:

- 2
- ☐ (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - ☐ (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 1
- ☒ (a) Encryption / le chiffrement
  - (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 1
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 1
- (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - ☒ (c) substitutions / des substitutions
  - (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- ☒ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - ☒ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 1
- (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques



## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- ☒ (a) Encryption / le chiffrement
- ☐ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
- ☒ (c) Digital signature / la signature numérique
- ☐ (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
- ☐ (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
- ☒ (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
- ☐ (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- ☒ (a) permutations / des permutations
- ☐ (b) corruptions / des corruptions
- ☒ (c) substitutions / des substitutions
- ☒ (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- ☒ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
- ☐ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
- ☒ (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
- ☒ (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- ☐ (a) often improves usability / améliore souvent l'utilisabilité
- ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
- ☒ (c) must rely on secret countermeasures / doit s'appuyer sur des contre-mesures secrètes
- ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 1
- (a) Encryption / le chiffrement
  - ☒ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 1
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - ☒ (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 1
- ☒ (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - (c) substitutions / des substitutions
  - ☒ (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- ☒ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - ☒ (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 1
- (a) often improves usability / améliore souvent l'utilisabilité
  - (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 2
- ☒ (a) Encryption / le chiffrement
  - ☒ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 2
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - ☒ (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 0
- (a) permutations / des permutations
  - ☒ (b) corruptions / des corruptions
  - (c) substitutions / des substitutions
  - ☒ (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - ☒ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 1
- ☒ (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - ☒ (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques



## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Écrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 0
- (a) Encryption / le chiffrement
  - (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - ☒ (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 1
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 1
- ☒ (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - ☒ (c) substitutions / des substitutions
  - ☒ (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 2
- (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 1
- (a) Encryption / le chiffrement
  - ☒ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 2
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - ☒ (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 1
- (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - ☒ (c) substitutions / des substitutions
  - (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - ☒ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 1
- (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

Name, Firstname / Nom, Prénom : ..... COSTA Renaud .....

3/10

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 2
- ☒ (a) Encryption / le chiffrement
  - ☐ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - ☐ (c) Digital signature / la signature numérique
  - ☐ (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 1
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - ☐ (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - ☐ (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - ☐ (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 0
- ☐ (a) permutations / des permutations
  - ☒ (b) corruptions / des corruptions
  - ☐ (c) substitutions / des substitutions
  - ☐ (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- ☐ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - ☐ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - ☐ (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - ☐ (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 0
- ☐ (a) often improves usability / améliore souvent l'utilisabilité
  - ☐ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - ☒ (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☐ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- ☒ (a) Encryption / le chiffrement
- ☐ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
- ☐ (c) Digital signature / la signature numérique
- ☐ (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
- ☐ (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
- ☐ (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
- ☐ (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- ☒ (a) permutations / des permutations
- ☐ (b) corruptions / des corruptions
- ☐ (c) substitutions / des substitutions
- ☐ (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- ☒ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
- ☐ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
- ☐ (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
- ☐ (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- ☒ (a) often improves usability / améliore souvent l'utilisabilité
- ☐ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
- ☐ (c) must rely on secret countermeasures / doit s'appuyer sur des contre-mesures secrètes
- ☐ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 1
- ☒ (a) Encryption / le chiffrement
  - ☐ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - ☐ (c) Digital signature / la signature numérique
  - ☐ (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 0
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - ☐ (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - ☐ (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - ☐ (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 1
- ☒ (a) permutations / des permutations
  - ☐ (b) corruptions / des corruptions
  - ☐ (c) substitutions / des substitutions
  - ☐ (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 2
- ☒ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - ☐ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - ☐ (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - ☐ (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 1
- ☐ (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - ☐ (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☐ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques



## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- (a) Encryption / le chiffrement
- (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
- (c) Digital signature / la signature numérique
- (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
- (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
- (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
- (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- (a) permutations / des permutations
- (b) corruptions / des corruptions
- (c) substitutions / des substitutions
- (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
- (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
- (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
- (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- (a) often improves usability / améliore souvent l'utilisabilité
- (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
- (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
- (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 1
- ☒ (a) Encryption / le chiffrement
  - ☐ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - ☐ (c) Digital signature / la signature numérique
  - ☐ (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 1
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - ☐ (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - ☐ (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - ☐ (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 0
- ☒ (a) permutations / des permutations
  - ☐ (b) corruptions / des corruptions
  - ☐ (c) substitutions / des substitutions
  - ☐ (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- ☐ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - ☒ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - ☐ (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - ☐ (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 2
- ☐ (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - ☐ (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☐ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

Name, Firstname / Nom, Prénom : ..... FLAMENT Maxime .....

5/10

## Software Security – Sécurité Logicielle Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point

### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 2
- ☒ (a) Encryption / le chiffrement
  - ☒ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

### Question 2 (2 points)

Digital signature : / La signature numérique :

- 1
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - (d) may use hash functions / peut utiliser des fonctions de hachage

### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 0
- (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - (c) substitutions / des substitutions
  - (d) transpositions / des transpositions

### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- ☒ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - ☒ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

### Question 5 (2 points)

Security: / La sécurité:

- 2
- (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 2
- ☒ (a) Encryption / le chiffrement
  - ☒ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 2
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - ☒ (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 0
- (a) permutations / des permutations
  - ☒ (b) corruptions / des corruptions
  - (c) substitutions / des substitutions
  - ☒ (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - ☒ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 1
- (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques



## Software Security – Sécurité Logicielle Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- ☒ (a) Encryption / le chiffrement
- ☐ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
- ☐ (c) Digital signature / la signature numérique
- ☐ (d) Hash functions / les fonctions de hachage

### Question 2 (2 points)

Digital signature : / La signature numérique :

- ☐ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
- ☐ (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
- ☐ (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
- ☒ (d) may use hash functions / peut utiliser des fonctions de hachage

### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- ☒ (a) permutations / des permutations
- ☐ (b) corruptions / des corruptions
- ☒ (c) substitutions / des substitutions
- ☐ (d) transpositions / des transpositions

### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- ☐ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
- ☐ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
- ☐ (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
- ☐ (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

### Question 5 (2 points)

Security: / La sécurité:

- ☐ (a) often improves usability / améliore souvent l'utilisabilité
- ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
- ☐ (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
- ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques



## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Écrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peut(ven)t directement implanter le service de Confidentialité ?

- 1
- ☒ (a) Encryption / le chiffrement
  - (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 1
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 2
- ☒ (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - ☒ (c) substitutions / des substitutions
  - (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - ☒ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - ☒ (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 1
- (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - ☒ (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

Name, Firstname / Nom, Prénom : ..G.O.N.N.I.N... ..ehant.....

9/10

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- (a) Encryption / le chiffrement
- (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
- (c) Digital signature / la signature numérique
- (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
- (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
- (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
- (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- (a) permutations / des permutations
- (b) corruptions / des corruptions
- (c) substitutions / des substitutions
- (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
- (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
- (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
- (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- (a) often improves usability / améliore souvent l'utilisabilité
- (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
- (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
- (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf 3ème temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 1
- (a) Encryption / le chiffrement
  - (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 1
- (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 2
- (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - (c) substitutions / des substitutions
  - (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 1
- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 2
- (a) often improves usability / améliore souvent l'utilisabilité
  - (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 1
- (a) Encryption / le chiffrement
  - (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 1
- (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 2
- (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - (c) substitutions / des substitutions
  - (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 2
- (a) often improves usability / améliore souvent l'utilisabilité
  - (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / *Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.*
- No exchange (eraser, pen, responses ...) is allowed between students / *Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit*
- You must switch off your mobile phone and store it into your bag / *Vous devez éteindre votre téléphone portable et le ranger dans votre sac*
- You have 9 minutes (except 3rd of time : 12 minutes) / *Vous avez 9 minutes (sauf tiers temps: 12 minutes)*
- Write your name, firstname, and group on every sheet / *Ecrivez nom, prénom et groupe sur chaque feuille*
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. *Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.*
- Selecting an incorrect answer will reduce the grade by 1 point. *Entourer une réponse incorrecte réduit la note de 1 point.*

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / *Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?*

- 1
- ☒ (a) Encryption / *le chiffrement*
  - ☐ (b) Privacy enforcement techniques / *les mécanismes de protection de la vie privée*
  - ☐ (c) Digital signature / *la signature numérique*
  - ☐ (d) Hash functions / *les fonctions de hachage*

#### Question 2 (2 points)

Digital signature : / *La signature numérique :*

- 0
- ☒ (a) can ensure the non-repudiation of origin / *peut assurer la non-répudiation d'origine*
  - ☐ (b) can ensure the non-repudiation of destination / *peut assurer la non-répudiation de destination*
  - ☐ (c) relies on symmetric encryption / *s'appuie sur le chiffrement symétrique*
  - ☐ (d) may use hash functions / *peut utiliser des fonctions de hachage*

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / *Les chiffres symétriques peuvent s'appuyer sur :*

- 1
- ☒ (a) permutations / *des permutations*
  - ☐ (b) corruptions / *des corruptions*
  - ☐ (c) substitutions / *des substitutions*
  - ☐ (d) transpositions / *des transpositions*

#### Question 4 (2 points)

For block ciphers: / *Pour des chiffrements par blocs:*

- 0
- ☐ (a) CBC mode offers a good protection / *le mode CBC offre une bonne protection*
  - ☐ (b) ECB mode offers a good protection / *le mode ECB offre une bonne protection*
  - ☐ (c) CTR mode offers a good protection / *le mode CTR offre une bonne protection*
  - ☒ (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / *le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré*

#### Question 5 (2 points)

Security: / *La sécurité:*

- 1
- ☐ (a) often improves usability / *améliore souvent l'utilisabilité*
  - ☐ (b) may introduce new vulnerabilities / *peut introduire de nouvelles vulnérabilités*
  - ☐ (c) must rely on secret countermeasures / *soit s'appuyer sur des contre-mesures secrètes*
  - ☒ (d) aims at reducing risks to assets / *visé à réduire les risques sur le capital et ressources informatiques*



Name, Firstname / Nom, Prénom : HUANG Shiyang

4/10

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 1
- ☒ (a) Encryption / le chiffrement
  - (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 0
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - ☒ (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 0
- ☒ (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - (c) substitutions / des substitutions
  - ☒ (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 1
- ☒ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 2
- (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Écrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- ☒ (a) Encryption / le chiffrement
- ☐ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
- ☒ (c) Digital signature / la signature numérique
- ☐ (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
- ☐ (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
- ☐ (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
- ☐ (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- ☒ (a) permutations / des permutations
- ☐ (b) corruptions / des corruptions
- ☐ (c) substitutions / des substitutions
- ☒ (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- ☒ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
- ☐ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
- ☐ (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
- ☐ (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- ☐ (a) often improves usability / améliore souvent l'utilisabilité
- ☐ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
- ☐ (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
- ☐ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

Name, Firstname / Nom, Prénom : ..... Kauffmann Elliot ..... 5/10

## Software Security – Sécurité Logicielle Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 1
- ☒ (a) Encryption / le chiffrement
  - ☐ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - ☐ (c) Digital signature / la signature numérique
  - ☐ (d) Hash functions / les fonctions de hachage

### Question 2 (2 points)

Digital signature : / La signature numérique :

- 0
- ☐ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - ☒ (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - ☒ (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - ☒ (d) may use hash functions / peut utiliser des fonctions de hachage

### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 2
- ☒ (a) permutations / des permutations
  - ☐ (b) corruptions / des corruptions
  - ☒ (c) substitutions / des substitutions
  - ☐ (d) transpositions / des transpositions

### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- ☐ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - ☒ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - ☒ (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - ☐ (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

### Question 5 (2 points)

Security: / La sécurité:

- 2
- ☐ (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - ☐ (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 1
- ☒ (a) Encryption / le chiffrement
  - (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 0
- (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - ☒ (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - ☒ (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 0
- (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - (c) substitutions / des substitutions
  - ☒ (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 1
- (a) often improves usability / améliore souvent l'utilisabilité
  - (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques



## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 2
- ☒ (a) Encryption / le chiffrement
  - ☒ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 2
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - ☒ (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 2
- ☒ (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - ☒ (c) substitutions / des substitutions
  - (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - ☒ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 1
- (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques



## Software Security – Sécurité Logicielle Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Écrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 1
- ☒ (a) Encryption / le chiffrement
  - ☒ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - (c) Digital signature / la signature numérique
  - ☒ (d) Hash functions / les fonctions de hachage

### Question 2 (2 points)

Digital signature : / La signature numérique :

- 1
- (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - ☒ (d) may use hash functions / peut utiliser des fonctions de hachage

### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 0
- (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - (c) substitutions / des substitutions
  - ☒ (d) transpositions / des transpositions

### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

### Question 5 (2 points)

Security: / La sécurité:

- 0
- (a) often improves usability / améliore souvent l'utilisabilité
  - (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - ☒ (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 2
- ☒ (a) Encryption / le chiffrement
  - ☒ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 2
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - ☒ (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 0
- ☒ (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - (c) substitutions / des substitutions
  - ☒ (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - ☒ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 0
- (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - ☒ (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 0
- (a) Encryption / le chiffrement
  - (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - ☒ (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 1
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 1
- ☒ (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - (c) substitutions / des substitutions
  - (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - ☒ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 2
- (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- (a) Encryption / le chiffrement
- (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
- (c) Digital signature / la signature numérique
- (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
- (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
- (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
- (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- (a) permutations / des permutations
- (b) corruptions / des corruptions
- (c) substitutions / des substitutions
- (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
- (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
- (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
- (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- (a) often improves usability / améliore souvent l'utilisabilité
- (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
- (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
- (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Écrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 1
- ☒ (a) Encryption / le chiffrement
  - (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 1
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 2
- ☒ (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - ☒ (c) substitutions / des substitutions
  - (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 0
- ☒ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - ☒ (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 1
- (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques



## Software Security – Sécurité Logicielle Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 2
- ☒ (a) Encryption / le chiffrement
  - ☐ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - ☐ (c) Digital signature / la signature numérique
  - ☐ (d) Hash functions / les fonctions de hachage

### Question 2 (2 points)

Digital signature : / La signature numérique :

- 1
- ☒ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - ☐ (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - ☐ (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - ☐ (d) may use hash functions / peut utiliser des fonctions de hachage

### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 2
- ☒ (a) permutations / des permutations
  - ☐ (b) corruptions / des corruptions
  - ☐ (c) substitutions / des substitutions
  - ☐ (d) transpositions / des transpositions

### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 1
- ☒ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - ☐ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - ☐ (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - ☐ (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

### Question 5 (2 points)

Security: / La sécurité:

- 2
- ☐ (a) often improves usability / améliore souvent l'utilisabilité
  - ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - ☐ (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- ☒ (a) Encryption / le chiffrement
- ☐ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
- ☒ (c) Digital signature / la signature numérique
- ☐ (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- ☐ (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
- ☒ (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
- ☒ (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
- ☐ (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- ☒ (a) permutations / des permutations
- ☐ (b) corruptions / des corruptions
- ☒ (c) substitutions / des substitutions
- ☒ (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- ☒ (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
- ☐ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
- ☐ (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
- ☐ (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- ☐ (a) often improves usability / améliore souvent l'utilisabilité
- ☒ (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
- ☒ (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
- ☐ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

Name, Firstname / Nom, Prénom : Roussau Nikita

3/10

## Software Security – Sécurité Logicielle Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- (a) Encryption / le chiffrement
- (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
- (c) Digital signature / la signature numérique
- (d) Hash functions / les fonctions de hachage

### Question 2 (2 points)

Digital signature : / La signature numérique :

- (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
- (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
- (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
- (d) may use hash functions / peut utiliser des fonctions de hachage

### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- (a) permutations / des permutations
- (b) corruptions / des corruptions
- (c) substitutions / des substitutions
- (d) transpositions / des transpositions

### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
- (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
- (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
- (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

### Question 5 (2 points)

Security: / La sécurité:

- (a) often improves usability / améliore souvent l'utilisabilité
- (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
- (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
- (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques

## Software Security – Sécurité Logicielle

### Quizz #3 – 06/12/2017

- You are not entitled to use the course, nor books, nor your personal notes, nor a calculator or computer for this examination / Vous n'avez droit à aucun document de cours, livre ou notes, ni calculatrice ou ordinateur.
- No exchange (eraser, pen, responses ...) is allowed between students / Tout échange entre étudiants (gomme, stylo, réponses ...) est interdit
- You must switch off your mobile phone and store it into your bag / Vous devez éteindre votre téléphone portable et le ranger dans votre sac
- You have 9 minutes (except 3rd of time : 12 minutes) / Vous avez 9 minutes (sauf tiers temps: 12 minutes)
- Write your name, firstname, and group on every sheet / Ecrivez nom, prénom et groupe sur chaque feuille
- Selecting all correct answers will bring the maximum grade for the question, and a fraction of these points according to the ratio of good answers. Entourer toutes les réponses correctes à une question apporte le nombre de points maximum, et une fraction de ces points au prorata des bonnes réponses sélectionnées.
- Selecting an incorrect answer will reduce the grade by 1 point. Entourer une réponse incorrecte réduit la note de 1 point.

#### Question 1 (2 points)

Which security mechanism(s) can directly implement the Confidentiality Service ? / Quel(s) mécanisme(s) de sécurité peu(ven)t directement implanter le service de Confidentialité ?

- 1
- ☒ (a) Encryption / le chiffrement
  - ☒ (b) Privacy enforcement techniques / les mécanismes de protection de la vie privée
  - ☒ (c) Digital signature / la signature numérique
  - (d) Hash functions / les fonctions de hachage

#### Question 2 (2 points)

Digital signature : / La signature numérique :

- 2
- (a) can ensure the non-repudiation of origin / peut assurer la non-répudiation d'origine
  - (b) can ensure the non-repudiation of destination / peut assurer la non-répudiation de destination
  - (c) relies on symmetric encryption / s'appuie sur le chiffrement symétrique
  - (d) may use hash functions / peut utiliser des fonctions de hachage

#### Question 3 (2 points)

Symmetric block ciphers may rely on: / Les chiffres symétriques peuvent s'appuyer sur :

- 2
- ☒ (a) permutations / des permutations
  - (b) corruptions / des corruptions
  - ☒ (c) substitutions / des substitutions
  - (d) transpositions / des transpositions

#### Question 4 (2 points)

For block ciphers: / Pour des chiffrements par blocs:

- 2
- (a) CBC mode offers a good protection / le mode CBC offre une bonne protection
  - ☒ (b) ECB mode offers a good protection / le mode ECB offre une bonne protection
  - (c) CTR mode offers a good protection / le mode CTR offre une bonne protection
  - (d) chaining always generates garbage cleartext after ciphertext blocks get corrupted then decrypted / le chaînage génère toujours un texte clair illisible après qu'un bloc chiffré soit corrompu puis déchiffré

#### Question 5 (2 points)

Security: / La sécurité:

- 2
- (a) often improves usability / améliore souvent l'utilisabilité
  - (b) may introduce new vulnerabilities / peut introduire de nouvelles vulnérabilités
  - ☒ (c) must rely on secret countermeasures / soit s'appuyer sur des contre-mesures secrètes
  - ☒ (d) aims at reducing risks to assets / vise à réduire les risques sur le capital et ressources informatiques