18 / 03 / 2024

Cryptographie et Sécurité - Contrôle continu

(durée : 2 heures)

Place : B1

Exercice 1

Soit $G : \{0,1\}^s \rightarrow \{0,1\}^n$ un générateur pseudo-aléatoire (PRG) sécurisé.

Question 1

Quels sont les PRG sécurisés parmi les suivants ? Dans tous les cas, précisez l'avantage de l'adversaire A.

1. $G'(k) = G(k) \oplus G(k)$
2. $G'(k) = \mathbf{reverse}(G(k))$

Question 2

Quelles sont les propositions incorrectes, parmi les suivantes ?

1. k est la graine du générateur
2. k est la clé publique
3. k est de taille n bits
4. k est utilisée pour le déchiffrement

Exercice 2

On considère le réseau S-P suivant : la taille de bloc est de **1 octet**, avec une S-box de **4 bits** pour chaque moitié du bloc. La P-box est décrite par une permutation sous la forme $(a, b, c, \ldots, p)$, où le bit a de l'entrée devient le bit b de la sortie, le bit b en entrée devient le bit c en sortie et ainsi de suite, jusqu'à ce que le bit p en entrée devienne le bit a en sortie.

S-Box :

in	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
out	B	8	7	A	C	E	1	3	4	0	F	6	9	5	D	2

P-Box : $(0, 2, 4, 7, 3, 5, 1, 6)$, les positions étant numérotées de gauche à droite

Question 1

Si l'entrée est `A6`, quelle est la valeur de l'octet de sortie après une seule ronde, en prenant en compte que la ronde se termine par un **XOR** avec une clé de ronde K_1 = `E5` ?

Question 2

Quelles sont les propositions incorrectes, parmi les suivantes ?

1. Les P-boxes introduisent de la confusion
2. AES est un réseau S-P
3. Rijndael est un réseau S-P
4. Les S-boxes introduisent de la linéarité

Exercice 3

On considère la courbe elliptique suivante : $y^2 \equiv x^3 + x + 3 \bmod 7$
La table d'addition des points de la courbe est donnée ci-dessous :

+	∞	(4,1)	(4,6)	(5,0)	(6,1)	(6,6)
∞	∞	(4,1)	(4,6)	(5,0)	(6,1)	(6,6)
(4,1)	(4,1)	(6,6)	∞	(6,1)	(4,6)	(5,0)
(4,6)	(4,6)	∞	(6,1)	(6,6)	(5,0)	(4,1)
(5,0)	(5,0)	(6,1)	(6,6)	∞	(4,1)	(4,6)
(6,1)	(6,1)	(4,6)	(5,0)	(4,1)	(6,6)	∞
(6,6)	(6,6)	(5,0)	(4,1)	(4,6)	∞	(6,1)

Question 1

Quel est l'ordre de la courbe elliptique ?

Question 2

Quels sont les éléments générateurs ? Formulez votre réponse sous la forme :
$(x_g, y_g) \rightarrow (x_{2g}, y_{2g}) \rightarrow \ldots \rightarrow O$

Question 3

Alice et Bob cherchent à établir un secret partagé via le protocole Diffie-Hellman. Ils utilisent cette courbe elliptique, avec comme générateur G le point de coordonnées $(4, 1)$. Le scalaire privé d'Alice est $a = 4$ et celui de Bob est $b = 1$.
Quelle est la valeur du secret partagé par Alice et Bob ?

18 / 03 / 2024

Cryptographie et Sécurité - Contrôle continu

(durée : 2 heures)

Place : B2

Exercice 1

Soit $G : \{0,1\}^s \to \{0,1\}^n$ un générateur pseudo-aléatoire (PRG) sécurisé.

Question 1

Quels sont les PRG sécurisés parmi les suivants ? Dans tous les cas, précisez l'avantage de l'adversaire A.

1. $G'(k) = G(k)[0, \ldots, n-2]$ (c.-à-d., les deux derniers bits sont tronqués)
2. $G'(k) = G(k) \oplus G(k)$

Question 2

Quelles sont les propositions incorrectes, parmi les suivantes ?

1. k est la clé secrète
2. k est la graine du générateur
3. k est de taille n bits
4. k n'est utilisée que pour le chiffrement

Exercice 2

On considère le réseau S-P suivant : la taille de bloc est de **1 octet**, avec une S-box de **4 bits** pour chaque moitié du bloc. La P-box est décrite par une permutation sous la forme $(a, b, c, \ldots, p)$, où le bit a de l'entrée devient le bit b de la sortie, le bit b en entrée devient le bit c en sortie et ainsi de suite, jusqu'à ce que le bit p en entrée devienne le bit a en sortie.

S-Box :

in	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
out	B	8	7	A	C	F	1	3	4	0	E	6	9	5	D	2

P-Box : $(0, 2, 4, 7, 3, 5, 1, 6)$, les positions étant numérotées de gauche à droite

Question 1

Si l'entrée est `A6`, quelle est la valeur de l'octet de sortie après une seule ronde, en prenant en compte que la ronde se termine par un **XOR** avec une clé de ronde K_1 = `E5` ?

Question 2

Quelles sont les propositions incorrectes, parmi les suivantes ?

1. Les P-boxes introduisent de la diffusion
2. DES est un réseau S-P
3. Rijndael est un réseau S-P
4. Les P-boxes introduisent de la non-linéarité

Exercice 3

On considère la courbe elliptique suivante : $y^2 \equiv x^3 + 2x + 1 \bmod 5$
La table d'addition des points de la courbe est donnée ci-dessous :

+	∞	(0,1)	(0,4)	(1,2)	(1,3)	(3,2)	(3,3)
∞	∞	(0,1)	(0,4)	(1,2)	(1,3)	(3,2)	(3,3)
(0,1)	(0,1)	(1,3)	∞	(0,4)	(3,3)	(1,2)	(3,2)
(0,4)	(0,4)	∞	(1,2)	(3,2)	(0,1)	(3,3)	(1,3)
(1,2)	(1,2)	(0,4)	(3,2)	(3,3)	∞	(1,3)	(0,1)
(1,3)	(1,3)	(3,3)	(0,1)	∞	(3,2)	(0,4)	(1,2)
(3,2)	(3,2)	(1,2)	(3,3)	(1,3)	(0,4)	(0,1)	∞
(3,3)	(3,3)	(3,2)	(1,3)	(0,1)	(1,2)	∞	(0,4)

Question 1

Quel est l'ordre de la courbe elliptique ?

Question 2

Quels sont les éléments générateurs ? Formulez votre réponse sous la forme :
$(x_g, y_g) \rightarrow (x_{2g}, y_{2g}) \rightarrow \ldots \rightarrow O$

Question 3

Alice et Bob cherchent à établir un secret partagé via le protocole Diffie-Hellman. Ils utilisent cette courbe elliptique, avec comme générateur G le point de coordonnées $(1, 2)$. Le scalaire privé d'Alice est $a = 2$ et celui de Bob est $b = 3$.
Quelle est la valeur du secret partagé par Alice et Bob ?

18 / 03 / 2024

Cryptographie et Sécurité - Contrôle continu

(durée : 2 heures)

Place : A1

Exercice 1

Soit $G : \{0,1\}^s \rightarrow \{0,1\}^n$ un générateur pseudo-aléatoire (PRG) sécurisé.

Question 1

Quels sont les PRG sécurisés parmi les suivants ? Dans tous les cas, précisez l'avantage de l'adversaire A.

1. $G'(k) = G(k) \| 0$ ($\|$ est la concaténation)
2. $G'(k) = \mathbf{reverse}(G(k))$

Question 2

Quelles sont les propositions correctes, parmi les suivantes ?

1. k est la graine du générateur
2. k est la clé publique
3. k est de taille n bits
4. k est utilisée pour le déchiffrement

Exercice 2

On considère le réseau S-P suivant : la taille de bloc est de **1 octet**, avec une S-box de **4 bits** pour chaque moitié du bloc. La P-box est décrite par une permutation sous la forme $(a, b, c, \ldots, p)$, où le bit a de l'entrée devient le bit b de la sortie, le bit b en entrée devient le bit c en sortie et ainsi de suite, jusqu'à ce que le bit p en entrée devienne le bit a en sortie.

S-Box :

in	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
out	B	8	7	A	C	E	1	3	4	0	F	6	9	5	D	2

P-Box : $(0, 2, 4, 7, 3, 1, 5, 6)$, les positions étant numérotées de gauche à droite

Question 1

Si l'entrée est `A6`, quelle est la valeur de l'octet de sortie après une seule ronde, en prenant en compte que la ronde se termine par un **XOR** avec une clé de ronde K_1 = `E5` ?

Question 2

Quelles sont les propositions correctes, parmi les suivantes ?

1. Les P-boxes introduisent de la confusion
2. AES est un réseau S-P
3. Rijndael est un réseau S-P
4. Les S-boxes introduisent de la linéarité

Exercice 3

On considère la courbe elliptique suivante : $y^2 \equiv x^3 + x + 3 \bmod 7$
La table d'addition des points de la courbe est donnée ci-dessous :

+	∞	(4,1)	(4,6)	(5,0)	(6,1)	(6,6)
∞	∞	(4,1)	(4,6)	(5,0)	(6,1)	(6,6)
(4,1)	(4,1)	(6,6)	∞	(6,1)	(4,6)	(5,0)
(4,6)	(4,6)	∞	(6,1)	(6,6)	(5,0)	(4,1)
(5,0)	(5,0)	(6,1)	(6,6)	∞	(4,1)	(4,6)
(6,1)	(6,1)	(4,6)	(5,0)	(4,1)	(6,6)	∞
(6,6)	(6,6)	(5,0)	(4,1)	(4,6)	∞	(6,1)

Question 1

Quel est l'ordre du corps fini sur lequel la courbe est définie ?

Question 2

Quels sont les éléments générateurs ? Formulez votre réponse sous la forme :
$(x_g, y_g) \rightarrow (x_{2g}, y_{2g}) \rightarrow \ldots \rightarrow O$

Question 3

Alice et Bob cherchent à établir un secret partagé via le protocole Diffie-Hellman. Ils utilisent cette courbe elliptique, avec comme générateur G le point de coordonnées $(4, 1)$. Le scalaire privé d'Alice est $a = 2$ et celui de Bob est $b = 2$.
Quelle est la valeur du secret partagé par Alice et Bob ?

18 / 03 / 2024

Cryptographie et Sécurité - Contrôle continu

(durée : 2 heures)

Place : A2

Exercice 1

Soit $G : \{0,1\}^s \to \{0,1\}^n$ un générateur pseudo-aléatoire (PRG) sécurisé.

Question 1

Quels sont les PRG sécurisés parmi les suivants ? Dans tous les cas, précisez l'avantage de l'adversaire A.

1. $G'(k) = G(k)[0, \ldots, n-2]$ (c.-à-d., les deux derniers bits sont tronqués)
2. $G'(k) = G(k) \| 0$ ($\|$ est la concaténation)

Question 2

Quelles sont les propositions correctes, parmi les suivantes ?

1. k est la clé secrète
2. k est la graine du générateur
3. k est de taille n bits
4. k n'est utilisée que pour le chiffrement

Exercice 2

On considère le réseau S-P suivant : la taille de bloc est de **1 octet**, avec une S-box de **4 bits** pour chaque moitié du bloc. La P-box est décrite par une permutation sous la forme $(a, b, c, \ldots, p)$, où le bit a de l'entrée devient le bit b de la sortie, le bit b en entrée devient le bit c en sortie et ainsi de suite, jusqu'à ce que le bit p en entrée devienne le bit a en sortie.

S-Box :

in	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
out	B	8	7	A	C	F	1	3	4	0	E	6	9	5	D	2

P-Box : $(0, 2, 4, 7, 3, 1, 5, 6)$, les positions étant numérotées de gauche à droite

Question 1

Si l'entrée est `A6`, quelle est la valeur de l'octet de sortie après une seule ronde, en prenant en compte que la ronde se termine par un **XOR** avec une clé de ronde K_1 = `E5` ?

Question 2

Quelles sont les propositions correctes, parmi les suivantes ?

1. Les P-boxes introduisent de la diffusion
2. DES est un réseau S-P
3. Rijndael est un réseau S-P
4. Les P-boxes introduisent de la non-linéarité

Exercice 3

On considère la courbe elliptique suivante : $y^2 \equiv x^3 + 2x + 1 \bmod 5$
La table d'addition des points de la courbe est donnée ci-dessous :

+	∞	(0,1)	(0,4)	(1,2)	(1,3)	(3,2)	(3,3)
∞	∞	(0,1)	(0,4)	(1,2)	(1,3)	(3,2)	(3,3)
(0,1)	(0,1)	(1,3)	∞	(0,4)	(3,3)	(1,2)	(3,2)
(0,4)	(0,4)	∞	(1,2)	(3,2)	(0,1)	(3,3)	(1,3)
(1,2)	(1,2)	(0,4)	(3,2)	(3,3)	∞	(1,3)	(0,1)
(1,3)	(1,3)	(3,3)	(0,1)	∞	(3,2)	(0,4)	(1,2)
(3,2)	(3,2)	(1,2)	(3,3)	(1,3)	(0,4)	(0,1)	∞
(3,3)	(3,3)	(3,2)	(1,3)	(0,1)	(1,2)	∞	(0,4)

Question 1

Quel est l'ordre du corps fini sur lequel la courbe est définie ?

Question 2

Quels sont les éléments générateurs ? Formulez votre réponse sous la forme :
$(x_g, y_g) \rightarrow (x_{2g}, y_{2g}) \rightarrow \ldots \rightarrow O$

Question 3

Alice et Bob cherchent à établir un secret partagé via le protocole Diffie-Hellman. Ils utilisent cette courbe elliptique, avec comme générateur G le point de coordonnées $(1, 2)$. Le scalaire privé d'Alice est $a = 2$ et celui de Bob est $b = 2$.
Quelle est la valeur du secret partagé par Alice et Bob ?