AMUSEC

Nombre de participants : 37

1. L'AES fait partie des chiffrements de type symétrique.

19 bonnes réponses
sur 19 répondants

✓	Vrai	100%	19 votes
	Faux	0%	0 votes

2. De quel type de chiffrement est RSA ?

19 bonnes réponses
sur 19 répondants

	Symétrique	0%	0 votes
✓	Asymétrique	100%	19 votes
	Hybride	0%	0 votes

3. Un chiffrement par bloc est de type asymétrique.

15 bonnes réponses
sur 19 répondants

	Vrai	21%	4 votes
✓	Faux	79%	15 votes

4. De quel type est une fonction de hachage ?

20 bonnes réponses
sur 21 répondants

	Symétrique	5%	1 vote
	Asymétrique	0%	0 votes
✓	C'est plus compliqué que ça	95%	20 votes

5. Quelle est la signification de l'acronyme ZKP ?

22 bonnes réponses
sur 22 répondants

	Zorro-Keyless Protocols	0%	0 votes
	Zen-Kryptographic Proofs	0%	0 votes
	Zero-Key Protocols	0%	0 votes
✓	Zero-Knowledge Proofs	100%	22 votes
	Zeta-Kernel Paradigm	0%	0 votes

6. "Où est Charlie ?" n'est pas un exemple de IZKP.

15 bonnes réponses
sur 19 répondants

	Vrai	21%	4 votes
✓	Faux	79%	15 votes

7. Le Sudoku est un exemple de

16 bonnes réponses
sur 21 répondants

✓	IZKP	76%	16 votes
	NIZKP	0%	0 votes
	Des 2	24%	5 votes

8. La cave d'Ali-Baba est un exemple de NIZKP.

14 bonnes réponses
sur 20 répondants

	Vrai	30%	6 votes
✓	Faux	70%	14 votes

9. Les AOPs sont des primitives symétriques ou asymétriques ?

11 bonnes réponses
sur 20 répondants

✓	Symétriques	55%	11 votes
	Asymétriques	15%	3 votes
	Aucun des 2	30%	6 votes

10. A quel type de primitives appartient l'AES ?

4 bonnes réponses
sur 15 répondants

	Type I	47%	7 votes
	Type II	13%	2 votes
	Type III	13%	2 votes
✓	Aucun des 3	27%	4 votes

11. Peut-on utiliser l'AES pour les protocoles avancés ?

12 bonnes réponses
sur 18 répondants

	Oui, évidemment	6%	1 vote
✓	On pourrait, mais ce n'est pas recommandé	67%	12 votes
	Non, certainement pas	28%	5 votes

12. La multiplication scalaire est un type de contraintes R1CS.

12 bonnes réponses
sur 20 répondants

	Vrai	40%	8 votes
✓	Faux	60%	12 votes

13. Les additions importent lors du calcul des contraintes Plonk.

19 bonnes réponses
sur 21 répondants

✓	Vrai	90%	19 votes
	Faux	10%	2 votes

14. Les portes personnalisées réduisent les contraintes AIR.

11 bonnes réponses
sur 23 répondants

	Vrai	52%	12 votes
✓	Faux	48%	11 votes

15. Combien faut-il de contraintes R1CS pour vérifier y = 3 x + 1 ?

7 bonnes réponses
sur 21 répondants

✓	0	33%	7 votes
	1	43%	9 votes
	2	24%	5 votes
	3	0%	0 votes

16. Combien faut-il de contraintes R1CS pour vérifier y = 3 x^2 + x ?

18 bonnes réponses
sur 23 répondants

	0	0%	0 votes
✓	1	78%	18 votes
	2	17%	4 votes
	3	4%	1 vote

17. Comment obtenir le moins de contraintes R1CS pour vérifier y = (x+1)^2 ?

10 bonnes réponses sur 22 répondants

	En développant l'expression	23%	5 votes
	En factorisant l'expression	32%	7 votes
✓	C'est pareil	45%	10 votes

18. Selon l'ordre lexicographique, quelle inégalité est vraie ?

7 bonnes réponses sur 13 répondants

	x1 x2 < x2 x3	23%	3 votes
	x3 > x1^3	23%	3 votes
✓	x1 > x2^3	54%	7 votes

19. Selon l'ordre lexicographique inverse gradué, x1x2x3 > x4x5.

7 bonnes réponses sur 18 répondants

✓	Vrai	39%	7 votes
	Faux	61%	11 votes

20. Pourrait-on utiliser l'astuce des SPN sur Reinforced Concrete ?

14 bonnes réponses sur 21 répondants

	Oui	33%	7 votes
✓	Non	67%	14 votes

21. Est-il pertinent d'utiliser l'attaque FreeLunch pour Feistel-MiMC ?

7 bonnes réponses sur 17 répondants

	Oui car elle est très efficace	59%	10 votes
✓	Non car elle est trop compliquée	41%	7 votes