

## EGZAMIN

1. Co oznacza *atak z wybraną wiadomością* (na szyfr)? Jaka jest różnica między atakiem *adaptacyjnym* a *wsadowym*?
2. Jaka jest różnica między schematami *wwierzytelniania* a *schematami podpisu*? Jakie są przewagi schematów *wwierzytelniania* nad *schematami podpisu* i odwrotnie?
3. Ile jest reszt kwadratowych modulo  $n = pq$  (gdzie  $p$  i  $q$  są różnymi, nieparzystymi liczbami pierwszymi)? Odpowiedź krótko uzasadnij.
4. Załóżmy, że istnieją funkcje jednokierunkowe. Przypomnijmy że (nieformalnie mówiąc), funkcja jednokierunkowa, to taka funkcja  $f$ , że na podstawie  $f(x)$  trudno wydajnie obliczyć jakiegokolwiek  $x'$ , takie, że  $f(x) = f(x')$ . Czy to oznacza, że trudno wydajnie obliczyć pierwszy bit takiego  $x'$ ? Odpowiedź uzasadnij.
5. Podaj (nieformalną) definicję generatorów pseudolosowych.
6. Jaka jest rola funkcji haszującej w schematach podpisu? (To znaczy: po co haszujemy wiadomość przed wykonaniem operacji teoriolizbowej, np. w RSA?)
7. Jakie są zalety i wady modelu z losową wyrocznią.
8. Podaj algorytm działania ślepych podpisów RSA.
9. Co to są podpisy niezaprzeczone?
10. Jak jest (potencjalne) zastosowanie podpisów progowych? (Wystarczy podać jakiegokolwiek zastosowanie, byle miało sens).

## Uwagi:

- Egzamin trwa 2 godziny.
- Nie wolno korzystać z notatek.
- Można pisać odpowiedzi na różne pytania na tych samych kartkach (proszę jednak wyraźnie je od siebie oddzielić).