29.05.02

Kryptografia i bezpieczeństwo

WPPT 2002, informatyka inżynierska

Zadania przygotowawcze na kolokwium

1. Zaproponować metody generowania serii kluczy symetrycznych przy pomocy: (a) algorytmu szyfrowania symetrycznego, (b) funkcji hashującej.

2. Jak Alicja i Bob mogą wygenerować klucz 128-bitowy tak, aby żadne z nich nie mogło w znaczący sposób wpłynąć na wynik? Nie korzystać z algorytmu DH.

3. Jak podzielić klucz na części A, B, C, A',B', C' tak aby rekonstrukcja klucza możliwa była na podstawie co najmniej 2 z części A, B, C oraz co najmniej dwóch z cześci A', B', C'.

4. W schemacie podziału sekretu Shamira sekret koduje się jako wartość wielomianu w zerze. Czy można byłoby przechować wartość sekretu jako wartość dla argumentu 1?

5. Udowodnić, że w przypadku schematu Shamira podziału sekretu „2 z 3" znajomość jednej części sekretu nie daje żadnej informacji o sekrecie.

6. Oryginalny protokół challenge and response wymaga po jednej stronie generowania ciągów losowych. Co zrobić, gdy nie mamy generatora liczb losowych ani dobrego generatora pseudolosowego? Dysponujemy chipem realizującym funkcje kryptograficzne.

7. Uzasadnić dlaczego w protokole uwierzytelniania Schnorra praktycznie nie jest przekazywana żadna wiedza o sekrecie.

8. Protokół uwierzytelniania Schnorra może być z łatwością użyty jako metoda tworzenia podpisów cyfrowych. Alicja, podpisując, naśladuje oryginalny protokół, ale zamiast czekać na challenge Boba wylicza go jako MD5(m) dla podpisywanej wiadomości m. Alicja chce pojść dalej i pozbyć się wyliczania losowego k w pierwszym kroku protokołu: zamiast tego oblicza SHA-1(m). Dobrze robi? Dlaczego?

9. Jak musi wygladać rejestracja nowego użytkownika w systemie chronionym Kerberosem? Jaki efekt ma w takim systemie cofnięcie zegara? Do ilu komputerów należy się włamać, by móc uzyskać dostęp do określonego serwisu?

10. Czy dla SSL możliwy jest atak man-in-the-middle?

11. Czy dla ssh możliwy jest atak man-in-the-middle?

12. Porównać zawodność metod biometrycznych z zawodnością mechanizmu PIN-ów: możliwość akceptacji nieuprawnionej osoby, możliwość odrzucenia uprawnionej osoby.

13. W wielu protokołach komunikacyjnych uzgadnia się klucz szyfrowania symetrycznego, zaś bardzo rzadko klucze szyfrowania asymetrycznego. Dlaczego? (nie chodzi wcale o długość kluczy). Jak przerobić protokół w którym są uzgadniane klucze asymetryczne w taki, w którym uzgadniane sa jedynie klucze symetryczne?

14. Karty mikroprocesorowe Pepetek są używane do otrzymywania bezpłatnie kawy z automatów na Wydziale. Jak zaprojektować komunikację między kartą a automatem, aby tylko posiadacze kart Pepetek mogli pobrać kawę. Wiemy, że na kawę czychają studenci z sąsiedniego wydziału zaopatrzeni w sprzęt do podsłuchu komunikacji. Studenci Ci mogą też zdobyć i rozłożyć na części kartę Pepetek.

/-/ Mirosław Kutyłowski