18.12.02

KRYPTOGRAFIA I BEZP. KOMP.,
WPPT, INF. INŻ. 2002

Lista zadań nr 3

1. Załóżmy, że istnieją urzędy certyfikacji A, B, C, D, E. Zaprojektuj tak układ wydawanych certyfikatów w ramach certyfikacji wzajemnej, aby klient urzędu X mógł zweryfikować podpisy klienta urzędu Y (dla dowolnych X, Y $\in \{A, B, C, D, E\}$). Każdy klient ma kontakt jedynie ze swym urzędem certyfikacji.

2. Atak słownikowy na hasła w UNIXie polega na tym, że w gotowym pliku są hash-e dla popularnych haseł. Policz jaka byłaby praktyczna złożoność ataku słownikowego, gdyby nie było *soli*. Jaka byłaby złożoność tego ataku, gdyby sól była 20-bitowa?

3. Schemat Lamporta haseł jednorazowych bazuje na wartościach funkcji hashujących. Ale hasła jednorazowe dawane klientom są krótsze i nie są zapisane binarnie. Jak zmodyfikować schemat Lamporta aby hasła dawane klientom były krótkie. Stosowanie funkcji hashujących operujących na takich krótkich ciągach oczywiście nie wchodzi w grę, bo dałoby się ją odwracać.
Zadanie to wymaga pewnej twórczej inwencji. Ale spróbuj coś wymyśleć!

4. Wymyśl jakąś rozsądną procedurę przyporządkowywania PIN-ów czteroliterowych na podstawie kryptogramu 64-bitowego. Wszystkie PIN-y maja być mniej więcej równo prawdopodobne (by uniemożliwić takie ataki jak na karty EC do 1998 roku).

5. Czy można zbudować token kryptograficzny opierając się na funkcji hashującej (a nie szyfrowaniu symetrycznym jak to było pokazane na wykładzie)?
Zaprojektować token kryptograficzny z wykorzystaniem funkcji asymetrycznych tak aby przesyłany ciąg mógł stanowić dowód wykonania określonego zlecenia.

6. Co by się stało w schemacie autoryzacji Schnorra, gdyby jedna ze stron nie wybierała parametrów losowo, ale w przewidywalny sposób. Przeanalizuj zagrożenia.

7. Podziel sekret 56 bitowy na 3 części zgodnie ze schematem opartym na wielomianach tak aby z dowolnych dwóch można było odzyskać całość. Zadbaj o wybór szczegółowych parametrów.

8. Dlaczego w schemacie podziału tajemnic k z n (oparty na wielomianach) przy znajomości $k-1$ kawałków sekretu nie da wykluczyć żadnej wartości sekretu? Znajdź przekonywujący argument matematyczny.

9. Czy w schemacie BBS bezpieczeństwo byłoby zagrożone, gdyby brać nie ostatnie bity a całe generowane liczby?

/-/ Mirosław Kutyłowski