27.10.02

Kryptografia i Bezp. Komp.,
WPPT, inf. inż. 2002

Lista zadań nr 2

1. Wyprowadź z pamięci wzory na deszyfrowanie w schemacie Feistela.

2. Dlaczego schemat kryptoanalizy różnicowej atakuje podklucze z ostatniej a nie z pierwszej rundy? Jak najsprawniej zdobyć pozostałe bity klucza, nie występujące w podkluczu ostatniej rundy?

3. Schematy budowy podkluczy, które komponowane są po prostu z jakichś ustalonych bitów klucza ułatwiają kryptograficzny. W jaki sposób?
Co możnaby zrobić by utrudnić tego typu atak? (wskazówka: jak użyć funkcji hashujących?)

4. Dlaczego dla RC5 zachodzi efekt lawinowy?

5. Który algorytm ma dłuższy klucz: DESX czy 3-DES? Jakie kłopoty możemy napotkać próbując zaimplementować kryptoanalizę różnicową dla tych algorytmów?

6. Wymienić te elementy DES-a, które czynią go stosunkowo wolnym w implementacjach na nie-dedykownym sprzęcie. Przemysleć, czy operacje Rijndaela nie stwarzają kłopotów w tym sensie.

/-/ Mirosław Kutyłowski