

**Egzamin z BSK, 3 lutego 2011 r.**

Imię i nazwisko: ..... Nr indeksu: .....

Odpowiedzi *tylko na temat* proszę pisać *wyraźnie* na otrzymanym formularzu.

1. [2 pkt.] Opisz jakiś schemat uzgadniania wspólnego tajnego klucza przez dwie strony komunikacji, nie faworyzujący żadnej ze stron.

2. [2 pkt.] Na czym podmiot uwierzytelniający może oprzeć przekonanie, że uwierzytelnia właściwego użytkownika?

3. [2 pkt.] Wymień, gdzie w SSH stosowane są szyfry asymetryczne, a gdzie symetryczne?

4. [2 pkt.] Dlaczego potrzebne są certyfikaty potwierdzające certyfikaty? Dlaczego certyfikaty tworzą hierarchię drzewiastą?

5. [2 pkt.] Jak można oszukać filtr sieciowy, wykorzystując mechanizm fragmentacji IP?

6. [2 pkt.] Wymień różnice między tunelowaniem za pomocą IPsec i SSL.

7. [2 pkt.] Jakie wady protokołu SMTP ułatwiają rozsyłanie spamu?
8. [2 pkt.] W jaki sposób RFID może naruszać prywatność użytkownika?
9. [2 pkt.] Jak generować losowość potrzebną w algorytmach kryptograficznych?
10. [2 pkt.] Wymień pożądane cechy kryptograficznej funkcji skrótu.
11. [2 pkt.] Opisz jakiś mechanizm pozwalający ominąć filtr sieciowy w płatnym punkcie dostępowym Wi-Fi.
12. [2 pkt.] Dlaczego stosuje się NAT?