Zagadnienia

PGP

1. W jakiej warstwie sieciowej działa PGP?
2. Przedstaw protokoł szyfrowania wiadomości wykorzystywany w PGP.
3. Przedstaw protokoł uwierzytelniania wiadomości wykorzystywany w PGP.
4. Przedstaw protokoł uwierzytelniania i szyfrowania wiadomości wykorzystywany w PGP.
5. Jakich usług dostarcza PGP?
6. W jaki sposób następuje uwierzytelnianie klucza publicznego w PGP?
7. Co to jest *Keyring*?
8. W jaki sposów przechowywany jest klucz prywatny w PGP?
9. W jakim celu PGP wykorzystuje protokół Diffie-Hellmana?
10. Czy Alice może posiadać wiele kluczy PGP? Jeśli tak to jak są one rozróżniane?

Standard certyfikatów X.509

1. Co to są certyfikaty? Jakich parametrów możemy uzyskać certyfikaty?
2. W jaki sposób certyfikaty rozwiązują *problem przynależności klucza publicznego do właściciela*?
3. Alice posiada parę k_A,K_A kluczy (prywatny i publiczny). Przedstaw protokół wydania certyfikatu klucza publicznego K_A przez CA (Certyfication Authority).
4. Alice i Bob posiadają certyfikaty swoich kluczy publicznych wydane przez CA_1 i CA_2, $CA_1 \neq CA_2$, odpowiednio Alice i Bobowi. Załóżmy, że Bob chce pobrać w bezpieczny sposób klucz publiczny Alice. Przedstaw odpowiedni protokół.
5. Co to są ścieżki (łańcuchy) certyfikatów?
6. Co to są listy CRL?
7. Jakie wartości (pola ceryfikacu) identyfikują właściciela certyfikatu?
8. Alice wygenerowała parę kluczy $K_A = (p, q, g, y)$ i $k_A = (p, q, x)$ do świadczenia usługi podpisu cyfowego DSA, gdzie K_A, k_A są odpowiednio jej kluczem publicznym i prywatnym. Przedstaw protokół, w którym Alice zgłasza sie do centrum CA w celu uzyskania certyfikatu pod swoim kluczem publicznym.

Protokół SLL

1. Jakie protokoły składają na protokół SSL?
2. Opisz SSL Record Protocol.
3. Jaką rolę spełnia SSL Change Cipher Specyfication Protocol?
4. Jakie rodzaje uwierzytelniania dostarcza SSL Handshake Protocol?
5. Jaki jest cel prototokołu Handshake? Jakie ustala parametry?
6. Alice wykorzystuje protokół SSL w celu połączenia się z serwerem S. Serwer S uwierzytelnia się za pomocą certyfikatu $X.509v3$ parametrów Diffiego-Hellmana $K = (y_s, g, p)$. Przedstaw fazę uzgadniania klucza protokołu SSL.
7. Alice wykorzystuje protokół SSL w celu połączenia się z serwerem S. Serwer S uwierzytelnia się za pomocą certyfikatu $X.509v3$ parametrów algorytmu RSA z opcją do szyfrowania $K = (n, e)$. Przedstaw fazę uzgadniania klucza protokołu SSL.
8. W jaki sposób klient uwierzytelnia się do serwera w protokole SSL? Przedstaw odpowiedni fragment protokołu.
9. W jakiej warstwie sieciowej działa protokół SSL?

Protokół Kerberos

1. W jakim celu stosujemy protokół Kerberos?
2. Jaki jest związek ataku słownikowego z protokołem Kerberos?
3. Przedstaw fazę protokołu Kerberos, w któwym następuje uwierzytelnienie użytkownika.
4. Alice wykorzystuje protokół *Kerberos* w celu uwierzytelnia się do servera S. Przedstaw mechanizm za pomocą, którego odpowiedni server *Kerberosa* uwierzytelnia się do Alice.
5. Alice wykonuje protokół *Kerberos*. W fazie II Alice uzyskała bilet T od servera TGS. Następnie Alice przeprowadza fazę III protokołu, w której zgłasza się z biletem T do servera V, w celu uzyskania dostępu do wybranej usługi na tym serwerze. Skąd Alice ma pewność, że kontaktuje się z V? Opisz odpowiedni mechanizm wykorzystywany w *Kerberosie*, który daje pewność Alice.
6. Alice chce uzyskać dostęp do pewnej usługi na serverze V. W tym celu uwierzytelnia się za pomocą protokółu *Kerberos*. W pierwszej fazie *Kerberosa* Alice uzyskuje bilet T od servera AS. Następnie Alice zgłasza się do servera TGS i wykorzystuje bilet T. Skąd wiadomo, że osoba posługująca się biletem jest osobą, której bilet został wydany? Opisz odpowiedni mechanizm wykorzystywany w *Kerberosie*.

7. Co to są królestwa Kerberosa?
8. W jakiej warstwie sieciowej działa protokół Kerberos?