Zadanie domowe 1

Uzupełnij główny tekst z użyciem akapitów zapisanych pod tekstem. Brakujące akapity wstaw w odpowiedniej (logicznej) kolejności.

Bezpieczeństwo połączenia WWW wynika najpierw z potwierdzenia autentyczności serwera WWW oraz z szyfrowania przesyłanych informacji (aby nikt niepowołany ich nie odczytał ani tym bardziej nie zmienił…).

Zacznijmy od końca...

Po potwierdzeniu autentyczności serwera przeglądarka internetowa ustala tzw. klucz sesji (czyli klucz szyfrowania) i od tej pory informacje przesyłane są w postaci zaszyfrowanej z zastosowaniem kryptografii symetrycznej.

W jaki sposób klucz sesji przesyłany jest do serwera WWW? Jako tekst jawny?

……

Nie! W żadnym wypadku! Do przesłania klucza sesji między przeglądarką a serwerem też używa się szyfrowania – stosuje się kryptografię asymetryczną!

……

Co to znaczy, że stosujemy kryptografię asymetryczną? Krótko mówiąc: Inny klucz używany jest do szyfrowania informacji, a inny odszyfrowania kryptogramu. Klucz służący do szyfrowania (nazywany publicznym) może być udostępniony publicznie, bo na jego podstawie nie da się w praktyce odtworzyć klucza prywatnego służącego do deszyfrowania.

……

Serwer udostępnia przeglądarce swój klucz publiczny (stanowi on element tzw. certyfikatu) i dopiero wówczas ta może przekazać w sposób bezpieczny klucz sesji, szyfrując go kluczem publicznym serwera.

Wracamy do początku…

Czy mamy jednak pewność, że serwer WWW, który przekazał swój klucz publiczny, był rzeczywiście tym, z którym miało być nawiązane połączenie? Odpowiedź brzmi: Nie! Użytkownik może stać się ofiarą tzw. ataku man-in-the-middle (problem tzw. *phishingu*).

……

Istnieje więc konieczność potwierdzenia autentyczności klucza publicznego! W jaki sposób się to dokonuje?

Otóż kluczowi publicznemu serwera WWW (właściwie całemu otrzymanemu od niego certyfikatowi) powinien towarzyszyć podpis cyfrowy jednej z zaufanych organizacji autoryzujących.

……

O podpisie cyfrowym…

Nadawca wiadomości tworzy tzw. skrót wiadomości, która ma być podpisana.

Skrót jest następnie szyfrowany kluczem… prywatnym twórcy wiadomości i jest załączany do oryginalnej wiadomości.

Odbiorca weryfikuje podpis postępując w następujący sposób: tworzy skrót odebranej wiadomości i porównuje go ze skrótem otrzymanym od nadawcy (oczywiście wcześniej musi go odszyfrować używając klucza… publicznego nadawcy).

……

A	Jeśli właściciel serwera sam o to nie zadba (tzn. nie uiści odpowiedniej opłaty), to wówczas przeglądarka nie jest w stanie potwierdzić autentyczności serwera WWW i pojawia się informacja o potencjalnym zagrożeniu. Możemy kontynuować, ale nie będzie pewności, że informacje trafią do odbiory (a nie jego klona).	D	Dla przykładu: W jednej z metod szyfrowania klucz publiczny jest, nieco upraszczając, iloczynem dwóch wielocyfrowych liczb pierwszych, które stanowią klucz prywatny – problem faktoryzacji jest tak złożony obliczeniowo, że nie da się w nieodległej przyszłości na podstawie klucza publicznego odtworzyć prywatnego.
B	Wówczas serwer imitujący zbiera wszelkie treści (np. loginy i hasła) od niezorientowanych użytkowników, które później będą wykorzystane np. na prawdziwej stronie banku.	E	Warto w tym momencie przypomnieć sobie, czym był klucz szyfrowania w szyfrze Cezara czy metodzie płotu – na czym polegał problem konieczności przekazania klucza szyfrowania?
C	Ta metoda nie jest tak szybka do zrealizowania (tzn. jest złożona obliczeniowo), więc nie jest stosowana do szyfrowania całego połączenia, a tylko na użytek przekazania klucza sesji.	F	W przypadku podpisu cyfrowego certyfikatu mamy do czynienia odpowiednio z kluczem prywatnym i publicznym organizacji autoryzującej (przeglądarki internetowe posiadają klucze publiczne wielu zaufanych organizacji autoryzujących).