**PROTOKÓŁ SSH**

Kolejny często wykorzystywany protokół warstwy aplikacji, to protokół zdalnego zarządzania hostami, zwany **SSH** (ang. Secure Shell). Dla osób nie zajmujących się informatyką na co dzień, nazwa ta niewiele mówi, ponieważ nie jest to protokół, którego używają “zwykli zjadacze chleba”, korzystający ze stron WWW czy też poczty elektronicznej. Stosowany jest on przez administratorów do **zarządzania serwerami** znajdującymi się bardzo często w różnych geograficznie miejscach, niekoniecznie w miejscu pracy. Stosują go też osoby, które mają np. wykupione **serwery VPS** i w ten sposób nimi administrują. Protokół ten wywodzi się z innego protokołu zdalnego dostępu, protokołu **TELNET** i jest jego, można powiedzieć lepszą wersją. Dlaczego? Dlatego, że TELNET, który notabene jest chyba najstarszym protokołem warstwy aplikacji, nie szyfruje komunikacji pomiędzy klientem a serwerem, komunikaty przesyłane są jawnym tekstem, a co za tym idzie istnieje możliwość przechwycenia komunikacji i podejrzenia jakie informacje są w sesji przesyłane. Ocenie jest to sytuacja nie do przyjęcia, dlatego też do zdalnego zarządzania hostami stosowany jest właśnie szyfrowany protokół SSH.



Domyślnym algorytmem szyfrowania komunikacji jest **algorytm RSA**, istnieje również możliwość szyfrowania danych za pomocą nieco słabszego **algorytmu DSA**. Podczas instalacji serwera SSH tworzona jest para kluczy – **klucz publiczny i prywatny** serwera – służą one do szyfrowania i deszyfrowania komunikacji. Podczas pierwszego połączenia z serwerem, klient, zapisuje publiczny klucz serwera na swoim dysku, w pliku **known\_hosts**.



Następnie tworzy tak zwany **klucz sesji**, który będzie stosowany do szyfrowania całej komunikacji. Klucz sesji zostaje zaszyfrowany kluczem publicznym otrzymanym wcześniej od serwera i jest do niego odsyłany. Od tego momentu cała komunikacja szyfrowana jest kluczem sesji.



Standardowo SSH działa na **porcie 22**. Jednym z najpopularniejszych programów klienckich wykorzystujących SSH, jest program **PUTTY**, jest darmowy i można go pobrać z sieci, a co więcej nie wymaga instalacji. Aby połączyć się zdalnie z hostem, wystarczy go uruchomić, podać nazwę hosta lub jego adres IP, wybrać SSH jeśli domyślnie nie jest zaznaczony i kliknąć OPEN. Jeśli po raz pierwszy łączymy się ze zdalnym hostem potwierdzamy chęć nawiązania połączenia i już możemy zdalnie nim zarządzać.

