

# Terminologia ochrony danych

<http://ipsec.pl/meta/terminologia-ochrony-danych.html>

{Polska terminologia komputerowa jest daleka od spójności i na jedno angielskie słowo przypada niekiedy po kilka tłumaczeń, jedno mniej zrozumiałe od drugiego. Poniżej chciałbym przedstawić wyjaśnienie znaczenia terminów związanych z kryptografią (ponieważ jest to leksykon), wraz z propozycjami ich tłumaczeń na język polski. Dodajmy że przedstawione propozycje są w większości zgodne z polskimi normami technicznymi dotyczącymi ochrony informacji (PN-I-02000).

{ idl;dt;strong;{authentication;/strong; i/dt;idd;

{Po polsku: ;strong;{uwierzytelnienie;/strong;. Słowo "uwierzytelnienie" oznacza potwierdzenie swojej tożsamości, stwierdzenie że dany podmiot jest tym, za kogo się podaje. A więc: podczas logowania do systemu uwierzytelniamy się przedstawiając mu dowody swojej tożsamości ({credentials) w postaci nazwy użytkownika ({login) i hasła. Słowo to pochodzi od potwierdzania "autentyczności" (patrz następny punkt), jednak w języku polskim raczej nie mówi się że osoba "jest autentyczna", stąd problemy z tłumaczeniem.

{Często spotykany w polskich tekstach potworek stanowiący kalke z angielskiego to słowo {autentykacja, czy jeszcze straszniejszy {autentyfikacja. Prosimy unikać. i/dd;dt;strong;{authenticity;/strong; i/dt;idd;

{Po polsku: ;strong;{autentyczność;/strong;. Określenia tego można użyć w odniesieniu do oprogramowania (pochodzące z zaufanego źródła, a więc autentyczne) i innych podmiotów nieosobowych. i/dd;dt;strong;{authorization, authorize;/strong; i/dt;idd;

{Po polsku: ;strong;{autoryzacja, autoryzować;/strong;. Słowo "autoryzować" oznacza potwierdzenie uprawnień lub uprawnienie kogoś do zrobienia czegoś. Na przykład centra autoryzacji kart kredytowych autoryzują transakcje nimi dokonywane. Słowo "autoryzacja" jest często mylone z {authentication. i/dd;dt;strong;{accounting;/strong; i/dt;idd;

{Po polsku: ;strong;{rozliczanie;/strong;, ostatecznie {billing. Słowo to oznacza czynności związane z rejestrowaniem aktywności (czasu pracy, ilości przesłanych danych) użytkownika. i/dd;dt;strong;{credentials;/strong; i/dt;idd;

{Słowo to oznacza dowody naszej tożsamości lub uprawnień. W zależności od kontekstu można go przetłumaczyć jako {uprawnienia, dowód tożsamości lub {dane uwierzytelniające. i/dd;dt;strong;{encryption, encrypt, encipher;/strong; i/dt;idd;

{Po polsku: ;strong;{szyfrowanie, szyfrować;/strong;. Niby oczywiste, ale spotyka się czasem mrożące krew w żyłach słowo {enkrypcja. i/dd;dt;strong;{decrypt, decipher;/strong; i/dt;idd;

{Po polsku: ;strong;{odszyfrować, rozszyfrować;/strong;. W starszych publikacjach spotyka się słowo {dekryptaż, które wywodzi się chyba z kregów wojskowych i brzmi naturalnie w określeniu takim jak np. "ośrodek dekryptażu w Bletchley Park". i/dd;dt;strong;{encode, decode;/strong; i/dt;idd;

{Po polsku: ;strong;{zakodować, odkodować, rozkodować;/strong;. Tłumaczenie tego słowa nie nastrecza nam jednak tylu problemów, co poprawne jego użycie: ;strong;{kodowanie nie jest tym samym co szyfrowanie;/strong;. W obu przypadkach przekształcamy jeden tekst na drugi przy pomocy jakiejś funkcji (szyfru lub kodu). Jednak w przypadku szyfrowania tekst wynikowy jest zależny od pewnego parametru tejże funkcji - tajnego klucza szyfrowania. W przypadku kodowania tekst jest przekształcany zawsze w taki sam sposób - kod nie posiada parametru (na dodatek tajnego), w przeciwieństwie do szyfru.

{Przykładem kodu może być kod ASCII, który każda literę koduje jako liczbę 0-255, kod Unicode, który każda literę koduje jako liczbę 0-65535 czy odmiana Unicode (ISO-10646), kodująca znaki jako liczby o długości 31 bitów.

{Dodajmy, że na temat różnic pomiędzy kodowaniem a szyfrowaniem można dyskutować wiele i zdaje sobie sprawę z licznych wyjątków oraz przypadków granicznych. Niemniej jednak uważam,

że przedstawione powyżej uproszczenia pozytywnie wpłyną na jednoznaczność polskich publikacji.

{Po polsku: `{hasło}`. Sprawa jest jasna w przypadku "password", ale duże zamieszanie w naszym języku wywołało słowo "passphrase". Różnica wynika stąd, że po angielsku "pass-word" znaczy tyle co "tajne słowo", co funkcjonowało dobrze kiedy hasła miały maksymalnie 8 znaków (<http://echelon.pl/leksykon/crypt.php>). Kiedy zaczęto stosować hasła o nieograniczonej długości, mogące być całymi zdaniami, zaczęto używać określenia "passphrase" ("tajne zdanie").

{W języku polskim zdaniem autora takie rozróżnienie nie jest konieczne, można co najwyżej zachęcić użytkownika do korzystania z hasła dłuższego niż 3 znaki i cyfra pisząc "Podaj długie hasło". Tak uczynił tłumacz polskiej wersji <http://www.gnupg.org/> GNU PG i jest to tłumaczenie zarówno zrozumiałe, jak i oddające sens angielskiego "passphrase".

{Po polsku: `{tekst jawny}`. Czyli najczęściej wiadomość przed zaszyfrowaniem lub po poprawnym rozszyfrowaniu.

{Po polsku: `{szyfrogram, kryptogram, tekst zaszyfrowany}`. To ostatnie określenie jest opisowe i tłumaczy jego znaczenie. W polskich normach dotyczących ochrony informacji stosuje się określenie "szyfrogram".

- {K. Gaj, K. Górski, A. Zugaj (Enigma), „Słowniczek terminów związanych z kryptologią i ochroną informacji angielsko - francusko - polski” <http://www.enigma.com.pl/konferencje/slowna kt1.html> > <http://www.enigma.com.pl/konferencje/slowna kt1.html> < /a > {Polski Komitet Normalizacyjny, {, ,Technika i Zabezpieczenia w systemach informatycznych – Terminologia" (PN – I – 02000)