Zakład Fizyki Budowli i Komputerowych Metod Projektowania
Instytut Budownictwa
Wydział Budownictwa Lądowego i Wodnego
Politechnika Wrocławska

Technologie informacyjne
- wykład 5 -

Prowadzący: dr inż. Łukasz Nowak, Grzegorz Dmochowski
Konsultacje: Pn C-7 9-11, Nd C-7 11-12,
Piątek, 15-16, s.13 ZOD JG
e-mail: g.dmochowski@pwr.wroc.pl
www: z2.ib.pwr.wroc.pl

Bezpieczeństwo systemów i zestawów informatycznych

dr inż. Łukasz Nowak, Grzegorz Dmochowski

Wymagania w zakresie poufności i dostępności danych

Systemy IT (ang. *information technology*) służą do wspomagania zarządzania informacją…

…czyli m.in. do ich gromadzenia, przechowywania, przetwarzania, udostępniania ...

Wymagania w zakresie poufności i dostępności danych

Informacja musi być:

- Poufna, do momentu gdy zostanie wykorzystana
- Wiarygodna dla nadawcy i adresata
- Dostępna we właściwym czasie i miejscu
- Niezaprzeczalna dla nadawcy i adresata

System IT musi wspomagać takie zarządzanie informacją aby spełniała ona powyższe warunki.

Wymagania w zakresie poufności i dostępności danych

Cechy bezpiecznego systemu IT:

- **Poufność**
  Ochrona przed ujawnieniem nieuprawnionemu odbiorcy
- **Integralność**
  Ochrona przed nieuprawniona modyfikacją lub zniekształceniem
- **Dostępność**
  Uprawniony dostęp do zasobów informacyjnych
- **Rozliczalność**
  Określenie i weryfikowanie odpowiedzialności za wykorzystanie systemu informacyjnego
- **Autentyczność**
  Weryfikacja tożsamości podmiotów i prawdziwości zasobów
- **Niezawodność**
  Gwarancja oczekiwanego zachowania systemu i otrzymywanych wyników

dr inż. Łukasz Nowak, Grzegorz Dmochowski

Cookies

- niewielkie informacje tekstowe, wysyłane przez serwer WWW i zapisywane po stronie użytkownika (zazwyczaj na twardym dysku)
- domyślne parametry ciasteczek pozwalają na odczytanie informacji w nich zawartych jedynie serwerowi, który je utworzył.
- są stosowane najczęściej w przypadku liczników, sond, sklepów internetowych, stron wymagających logowania, reklam i do monitorowania aktywności odwiedzających
- umożliwiają tworzenie spersonalizowanych serwisów WWW, obsługi logowania, "koszyków zakupowych" w internetowych sklepach itp.

dr inż. Łukasz Nowak, Grzegorz Dmochowski

Szacowanie ryzyka

Szacowanie ryzyka w systemie zarządzania bezpieczeństwem informacji zgodnym z ISO 27001

Zgodnie z wymaganiami normy ISO 27001 o wyborze odpowiedniego podejścia do szacowania ryzyka decyduje organizacja. Wybór metody powinien być odpowiedni w odniesieniu do prowadzonej przez organizację działalność i jej wymagania dotyczące bezpieczeństwa.

dr inż. Łukasz Nowak, Grzegorz Dmochowski

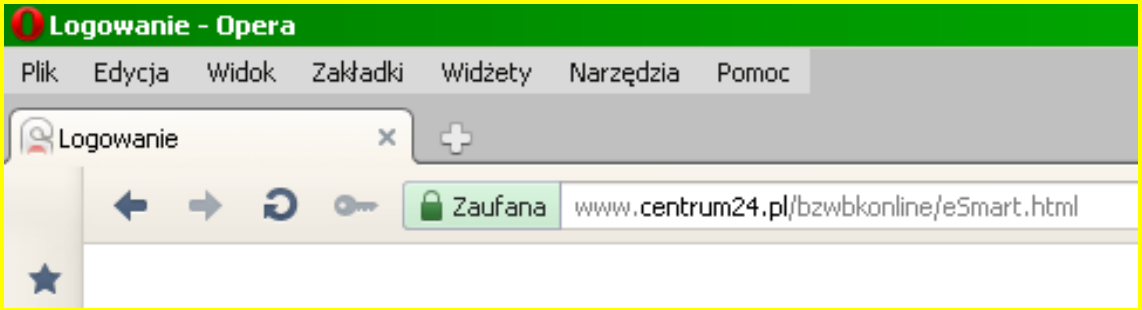
Procedury bezpieczeństwa 1/4

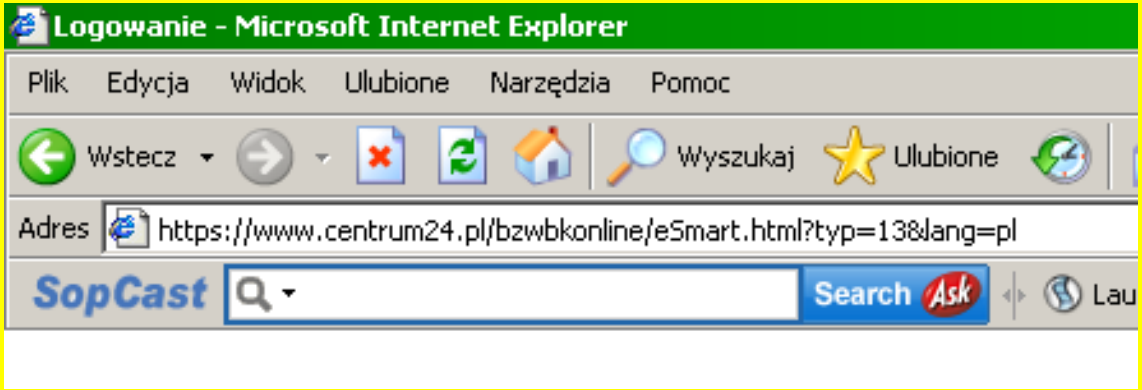
- **TLS (ang. *Transport Layer Security*) – przyjęty jako standard w Internecie, jest to rozwinięcie protokołu SSL (ang. *Secure Socket Layer*)**
- **SSL nie jest żadnym nowym algorytmem szyfrującym - to ustandaryzowany zestaw wcześniej znanych algorytmów, technik i schematów używanych do zapewnienia bezpieczeństwa. Wykorzystuje on algorytmy szyfrowania.**
- **SSL jest najczęściej kojarzony z protokołem HTTP (HTTPS), ale może służyć do zabezpieczania wielu innych protokołów, m.in.: Telnet, SMTP, POP, IMAP czy FTP, gdyż protokoły te same w sobie nie zapewniają szyfrowania transmisji.**

Procedury bezpieczeństwa 2/4

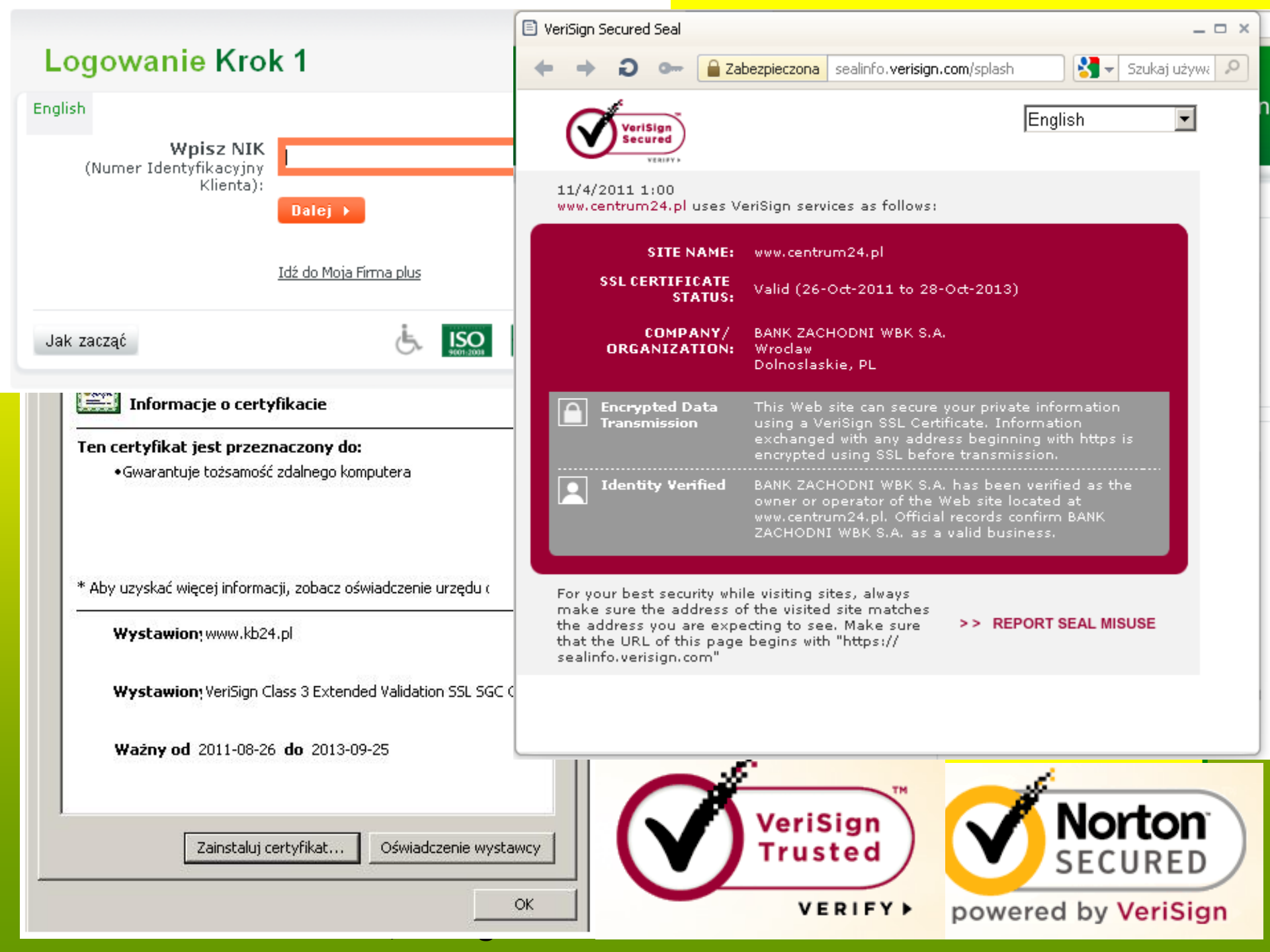
- **Krytycznym parametrem określającym siłę szyfrowania SSL jest długość użytych kluczy. Im dłuższy klucz, tym trudniej jest go złamać, a przez to odszyfrować transmisję.**
- **Dla kluczy asymetrycznych, zgodnie z zaleceniami organizacji NIST, długością sugerowaną jest obecnie 2048 bitów.**
- **Powszechnie używane są wyrażenia „SSL 128 bitów” oraz „SSL 40 bitów” określające długość użytego klucza symetrycznego.**

Procedury bezpieczeństwa 3/4





dr inż. Łukasz Nowak, Grzegorz Dmochowski


Logowanie Krok 1
English
Wpisz NIK
(Numer Identyfikacyjny Klienta):
Dalej
Idź do Moja Firma plus
Jak zacząć
ISO
VeriSign Secured Seal
Zabezpieczona
sealinfo.verisign.com/splash
Szukaj używa
VeriSign Secured
English
11/4/2011 1:00
www.centrum24.pl uses VeriSign services as follows:
SITE NAME: www.centrum24.pl
SSL CERTIFICATE STATUS: Valid (26-Oct-2011 to 28-Oct-2013)
COMPANY/ ORGANIZATION: BANK ZACHODNI WBK S.A.
Wroclaw
Dolnoslaskie, PL
Encrypted Data Transmission
This Web site can secure your private information using a VeriSign SSL Certificate. Information exchanged with any address beginning with https is encrypted using SSL before transmission.
Identity Verified
BANK ZACHODNI WBK S.A. has been verified as the owner or operator of the Web site located at www.centrum24.pl. Official records confirm BANK ZACHODNI WBK S.A. as a valid business.
For your best security while visiting sites, always make sure the address of the visited site matches the address you are expecting to see. Make sure that the URL of this page begins with "https://sealinfo.verisign.com"
>> REPORT SEAL MISUSE
Informacje o certyfikacie
Ten certyfikat jest przeznaczony do:
•Gwarantuje tożsamość zdalnego komputera
* Aby uzyskać więcej informacji, zobacz oświadczenie urzędu
Wystawion: www.kb24.pl
Wystawion: VeriSign Class 3 Extended Validation SSL SGC
Ważny od 2011-08-26 do 2013-09-25
Zainstaluj certyfikat...
Oświadczenie wystawcy
OK
VeriSign Trusted
VERIFY
Norton SECURED
powered by VeriSign

NCCert

Narodowe Centrum Certyfikacji – główny urząd certyfikacji (tzw. root) dla infrastruktury bezpiecznego podpisu elektronicznego w Polsce, prowadzony przez departament ochrony Narodowego Banku Polskiego.

Zadania

- **wytwarzanie i wydawanie zaświadczeń certyfikacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne**
- **prowadzenie rejestru tych podmiotów**

Hasło (password)

jest to ciąg znaków, które mogą być użyte w niektórych przypadkach uwierzytelniania

Hasła są często używane do uwierzytelniania tożsamości użytkownika systemu automatycznego przetwarzania danych i w niektórych przypadkach do udzielania lub odrzucenia dostępu do prywatnych lub wielodostępnych danych.

Wymagania haseł 1/3

Amerykański standard (*Federal Information Processing Standard*) nr 112 "Password Usage" specyfikuje podstawowe kryteria bezpieczeństwa dla użyć haseł w systemach przetwarzania danych:

1. Przedział długości

zbiór 95 znaków graficznych alfabetu ASCII, nie mniej niż 10 znaków

2. Zestaw

nie krótszy niż 4 znaki, dając minimum 10^4 możliwych haseł

3. Okres ważności

powinien zapewniać wymagany poziom ochrony przy najniższym możliwym koszcie

4. Źródło

hasła użytkownika sprawdzane przez system haseł, hasła generowane przez system - metoda generacji nie powinna być przewidywalna

dr inż. Łukasz Nowak, Grzegorz Dmochowski

Wymagania haseł 2/3

5. Własność

Osobiste hasło powinno być własnością indywidualną bardziej niż własnością wspólną grupy użytkowników z powodu gwarancji indywidualnej odpowiedzialności w systemie komputerowym

6. Dystrybucja

Inicjacyjne hasło jest tworzone i dostarczane podczas pierwszego spotkania na którym użytkownik inicjalizuje autoryzowane użycie systemu komputerowego lub dostęp do zbioru danych. Może być jednorazowe.

7. Pamiętanie

Hasła powinny być pamiętane w systemie uwierzytelniania w sposób który minimalizuje jego narażenie na odkrycie lub nieautoryzowaną zmianę.

Wymagania haseł 3/3

8. Wejście

Długie, przypadkowe hasło które jest trudne do wprowadzenia, może być bardziej wrażliwe na obserwację aniżeli krótkie, łatwo wprowadzalne hasło. W żadnym przypadku żadna drukowana czy wyświetlana kopia hasła nie powinna istnieć po wprowadzeniu hasła. Gdy hasło jest dostarczane jako część w procesie odległego wprowadzania, hasło powinno być dołączane do "przesyłki" w ostatnim możliwym momencie i fizycznie chronione.

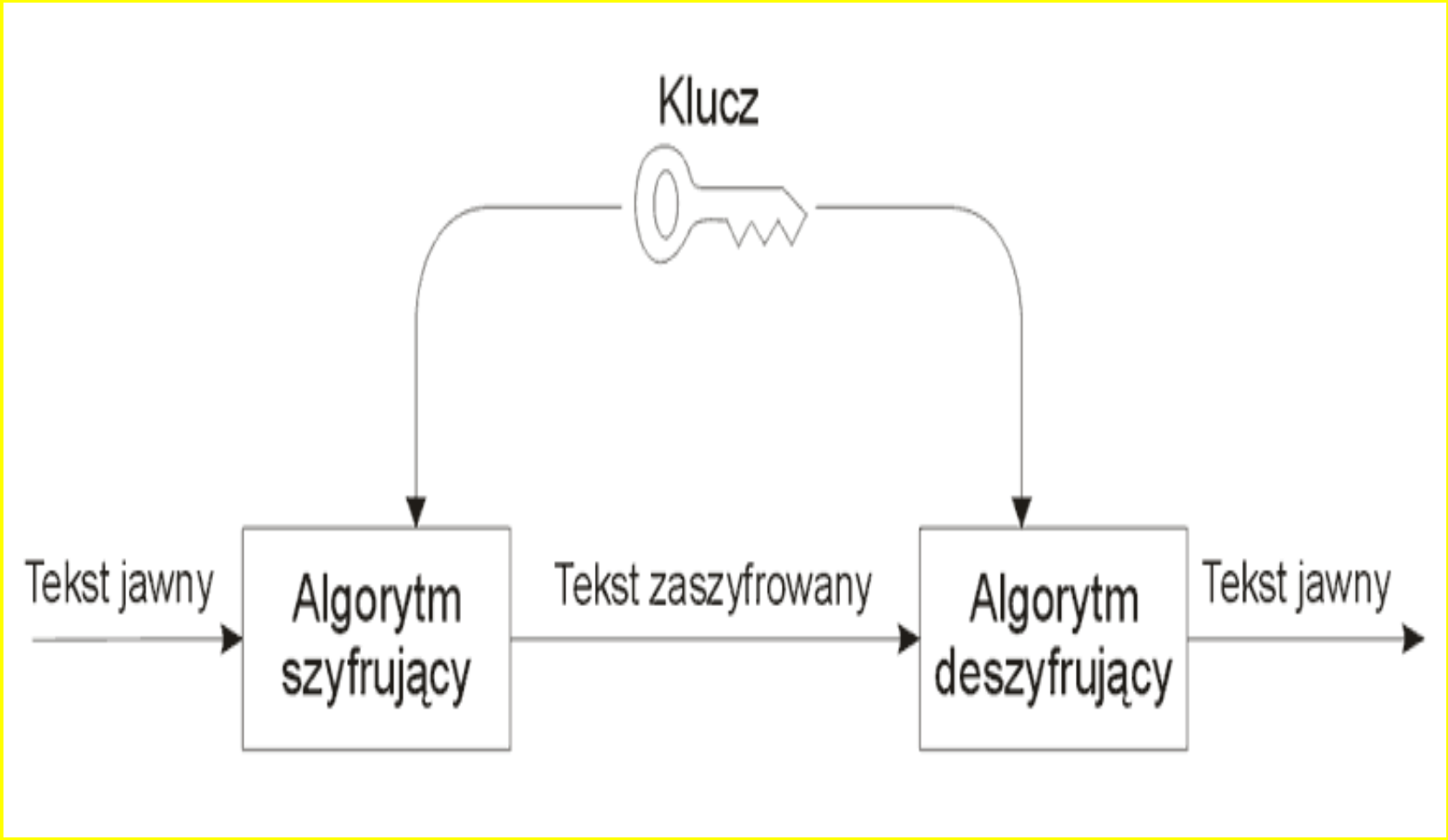
9. Transmisja

Większość linii komunikacyjnych między terminalami i komputerami nie zapewnia protekcji przed ujawnieniem hasła.

10. Okres uwierzytelniania

Ma to na celu zapobieżenie przed użyciem niepilnowanego terminala przez kogoś obcego

Systemy szyfrów - schemat



dr inż. Łukasz Nowak, Grzegorz Dmochowski

Systemy szyfrów - podział

Algorytmy szyfrowania dzielimy na:

- **symetryczne**
  - **do szyfrowania i deszyfrowania danych używany jest ten sam klucz,**
  - **znając klucz szyfrujący możemy dokonać również deszyfracji danych (wyznaczyć klucz deszyfrujący),**
- **asymetryczne (z kluczem publicznym)**
  - **do szyfrowania i deszyfrowania używane są różne klucze,**
  - **znając klucz szyfrujący nie możemy odszyfrować wiadomości (klucza deszyfrującego nie da się w prosty sposób wyznaczyć z klucza szyfrującego),**
  - **klucz służący do szyfrowania jest udostępniany publicznie (klucz publiczny), ale informację nim zakodowaną może odczytać jedynie posiadacz klucza deszyfrującego (klucz prywatny), który nie jest nikomu ujawniany.**

PGP (ang. *Pretty Good Privacy*)
Philip Zimmermann

Jedno z najpopularniejszych narzędzi do szyfrowania poczty elektronicznej

Ogólnie dostępny pakiet programowy do kodowania i podpisywania przesyłanych danych

Nadawca

- Koduje podpis własnym kluczem prywatnym
- Koduje podpisany komunikat kluczem publicznym odbiorcy

Odbiorca

- Dekoduje komunikat własnym kluczem prywatnym
- Dekoduje podpis kluczem publicznym nadawcy

dr inż. Łukasz Nowak, Grzegorz Dmochowski

X.509

- Koncepcja certyfikatów, ich ważności oraz odwoływania została przedstawiona po raz pierwszy w 1978 roku przez Lorena Kohnfeldra
- X.509 to standard definiujący schemat dla certyfikatów kluczy publicznych, unieważnień certyfikatów oraz certyfikatów atrybutu służących do budowania hierarchicznej struktury PKI (ang. *Public Key Infrastructure*)
- Kluczowym elementem jest urząd certyfikacji, który pełni rolę zaufanej trzeciej strony w stosunku do podmiotów oraz użytkowników certyfikatów.

Podpis elektroniczny

- pojęcie normatywne zdefiniowane w ustawie z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. z 2001 r. Nr 130, poz. 1450 z późn. zm),
- są to dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny,
- od strony technicznej podpis elektroniczny jest realizowany za pomocą mechanizmów podpisu cyfrowego
- najpopularniejsze standardy pozwalające na złożenie podpisu elektronicznego to X.509 oraz PGP

Po co podpis elektroniczny?

- **Zapewnienie autentyczności, czyli pewności co do autorstwa dokumentu,**
- **Zapewnienie niezaprzeczalności nadania informacji, nadawca wiadomości nie może wyprzeć się wysłania wiadomości, gdyż podpis cyfrowy stanowi dowód jej wysłania (istnieją także inne rodzaje niezaprzeczalności),**
- **Zapewnienie integralności, czyli pewności, że wiadomość nie została zmodyfikowana po złożeniu podpisu przez autora.**

Bezpieczny podpis elektroniczny

- **jest przyporządkowany wyłącznie do osoby składającej ten podpis,**
- **jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,**
- **jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.**

Rodzaje podpisu elektronicznego

Prawo unijne (dyrektywa 1999/93/EC) wyróżnia następujące rodzaje podpisu elektronicznego:

- **Podpis elektroniczny**

deklaracja tożsamości autora, złożona w formie elektronicznej pod dokumentem

- **Zaawansowany (bezpieczny) podpis elektroniczny**

podpis, który za pomocą odpowiednich środków technicznych (kryptograficznych) jest jednoznacznie i w sposób trudny do sfałszowania związany z dokumentem oraz autorem (wykorzystuje różne algorytmy kryptograficzne dla zapewnienia bezpieczeństwa)

- **Kwalifikowany podpis elektroniczny**

podpis złożony przy pomocy certyfikatu kwalifikowanego oraz przy użyciu bezpiecznego urządzenia do składania podpisu (SSCD)

Dziękuję za uwagę

Zakład Fizyki Budowli i Komputerowych Metod Projektowania
Instytut Budownictwa
Wydział Budownictwa Lądowego i Wodnego
Politechnika Wrocławska

Technologie informacyjne
- wykład 5 -

Prowadzący: dr inż. Łukasz Nowak, Grzegorz Dmochowski
Konsultacje: Pn C-7 9-11, Nd C-7 11-12,
Piątek, 15-16, s.13 ZOD JG
e-mail: g.dmochowski@pwr.wroc.pl
www: z2.ib.pwr.wroc.pl