Kryptografia i ochrona informacji

Protokoły kryptograficzne: projektowanie, analiza i zastosowanie w bezpiecznej komunikacji i usługach realizowanych drogą elektroniczną na przykładzie e-health.

Opiekun:
prof. dr hab. inż. Zbigniew Kotulski

Autor:
Magda Łyszczarz

Plan prezentacji

- Co to jest e-health?
- Cele pracy inżynierskiej
- Architektura aplikacji
- Zastosowane metody
  - Kod Hamminga
  - Podpis cyfrowy
- Aplikacja
- Dalsze plany
- Rozwój projektu
- Bibliografia

Co to jest e-health ?

- Różnego rodzaju aplikacje, rozwiązania i narzędzia integrujące środowisko: medyczne i telekomunikacyjne w zakresie polepszenia współpracy między personelem medycznym a pacjentami i ułatwieniu dostępu do opieki medycznej w państwie

Kierunki rozwoju e-healtha

- elektroniczne archiwum zdrowotne
- telemedycyna
- elektroniczny system obsługi pacjenta
- zdalna opieka medyczna
- technologie informacyjno-komunikacyjne w opiece zdrowotnej
- zarządzanie informacjami o zdrowiu
- informatyka medyczna

Dokąd zmierza e-health

- przenośne (osobiste) systemy do monitorowania stanu zdrowia
- usługi w zakresie telemedycyna (homecare)
- systemy pozwalające na szybki dostęp do najważniejszych danych medycznych i wymiany informacji o stanie zdrowia chorych

Korzyści płynące z e-healtha

- powstanie zintegrowanych systemów opieki medycznej, które są kluczową infrastrukturą związaną z opieką skierowaną na chorego
- wsparcie dla najnowszych metod diagnostycznych
- możliwość efektywniejszego śledzenia procedur medycznych
- poradzenie sobie z problem braku odpowiedniej obsługi medycznej poprzez śledzenie i identyfikowanie na bieżąco potrzeb pacjenta
- nowe sposoby powiadamiania o stanie zdrowia pacjenta za pomocą takich kanałów jak SMS, MMS, e-mail. Skutkuje to poprawą komunikacji pomiędzy lekarzem i pacjentem i jego krewnymi
- pomoc w realizacji procesów medycznych jak na przykład utworzenie aplikacji pozwalającej lekarzowi przepisującemu lekarstwa na podgląd aktualnej listy dostępnych leków

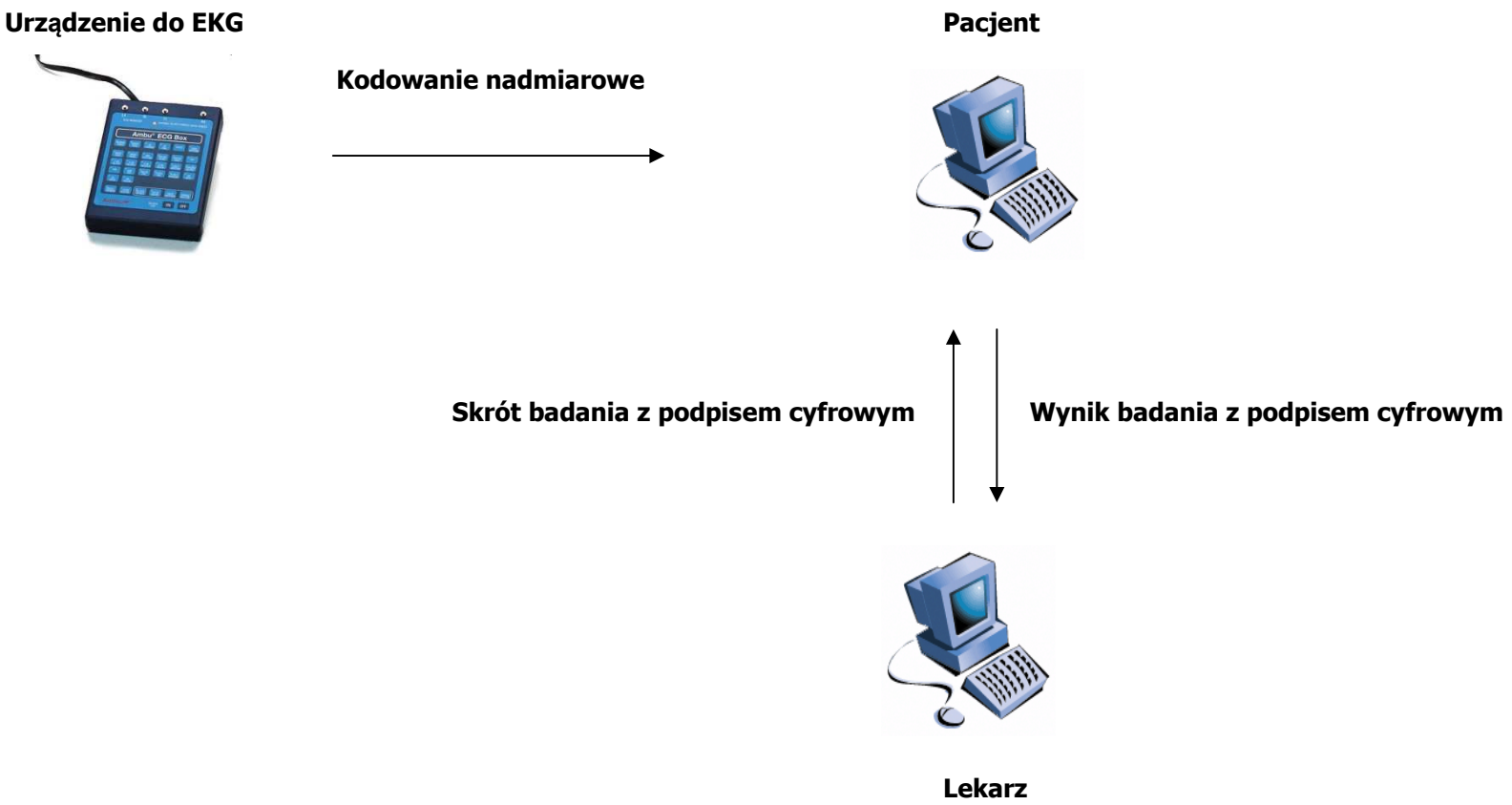
Potencjalne zagrożenia

- Bezpieczeństwo
  - nieautoryzowany dostęp do poufnych danych pacjenta oraz informacji klinicznych przez różnego rodzaju nieporządnych użytkowników podłączających się zdalnie do sieci bezprzewodowej
  - nieautoryzowany dostęp do danych za pomocą mobilnego urządzenia należącego do personelu medycznego
  - starta bądź kradzież urządzenia mobilnego zawierającego krytyczne i poufne dane
- brak standardów informacyjnych
- problem zapewnienia synchronizacji podczas przesyłania danych różnymi kanałami w tym samym czasie
- niejednoznaczne wymogi prawne
- problem zapewnienia prywatności w opiece klinicznej
- integracja medycyny, informatyki i telekomunikacji w celu zapewniania zgodności z systemami ochrony zdrowia na przykład takimi jak HL7

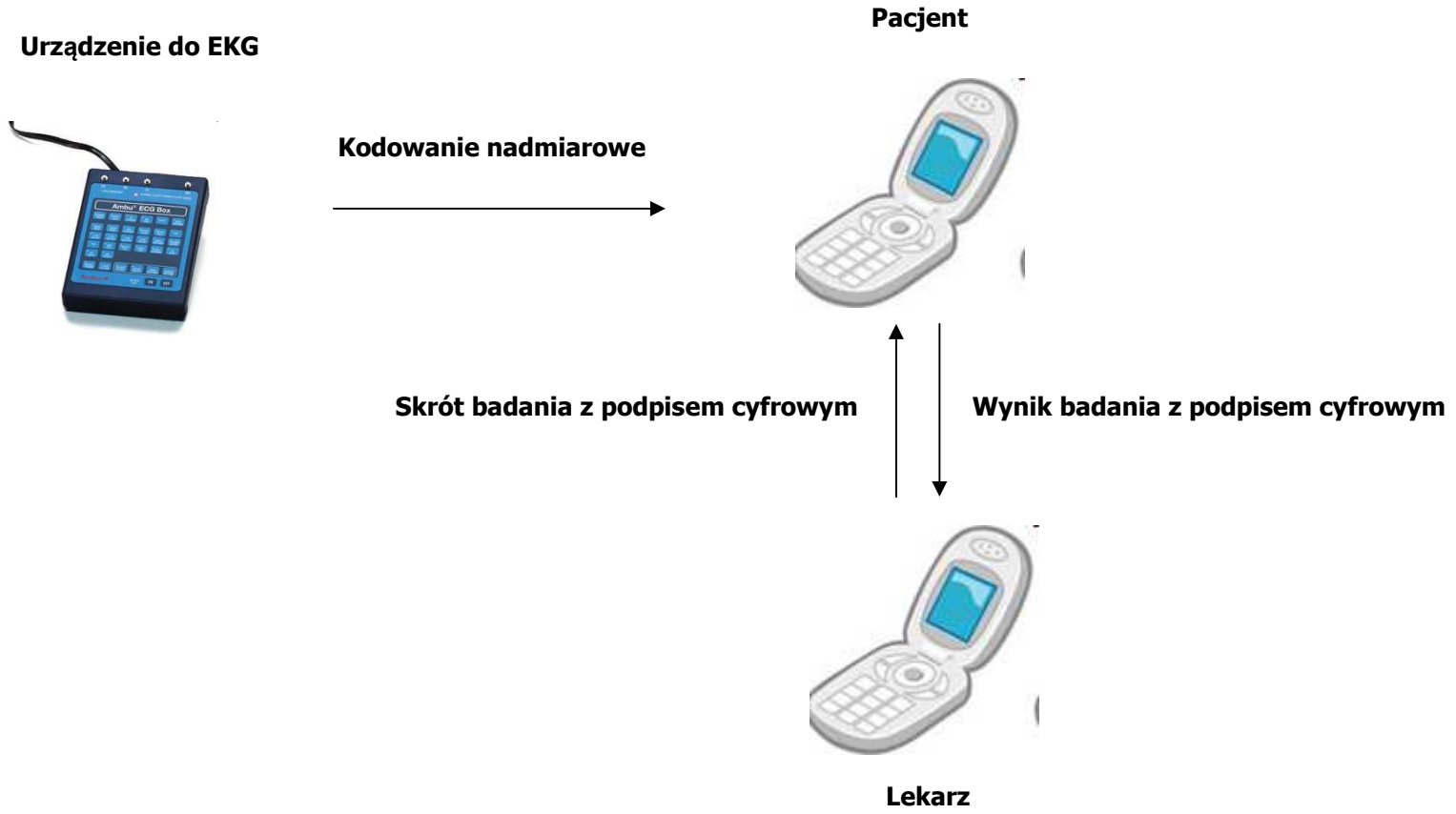
Cele pracy inżynierskiej

- Przedstawienie protokołów i algorytmów kryptograficznych służących do zapewnienia bezstratnej i bezpiecznej komunikacji drogą elektroniczną
- Wybór algorytmu do bezstratnej transmisji
- Wybór protokołów kryptograficznych do bezpiecznej transmisji
- Implementacja wybranych metod w aplikacji, w celu pokazania ich praktycznego zastosowania

Architektura aplikacji



Opcjonalna architektura aplikacji



Zastosowane metody (1/4)

W celu zapewnienia bezstratnego przekazu:

- Kodowanie nadmiarowe - kod Hamminga

W celu zapewnienia bezpieczeństwa:

- Logowanie do aplikacji
- Hasło jednorazowe wysyłane SMSem
- Funkcja skrótu
- Podpis cyfrowy

Kod Hamminga (7,4) (2/4)

- Kod z kontrolą parzystości
- Czterem bitom informacji opowiadają trzy bity korekcyjne
- Przykład: wysyłana wiadomość x=0110101

Obliczmy kod nadmiarowy dla wiadomości x=0110101.
Zapiszmy najpierw to słowo zostawiając miejsca na bity nadmiarowe:
__0_110_101
Obliczamy x_1: __**0**_**1**1**0**_1**01** ==> x_1=0+1+0+1+1=1
Obliczamy x_2: 1_**0**_1**10**_1**01** ==> x_2=0+1+0+0+1=0
Obliczamy x_4: 100_**110**_101 ==> x_4=1+1+0=0
Obliczamy x_8: 1000110_**101** ==> x_2=1+0+1=0
Zakodowana wiadomość: 10001100101
Kod nadmiarowy y: 1000

K. Tyl, Kodowanie nadmiarowe. Kod Hamminga.

Kod Hamminga (7,4) (3/4)

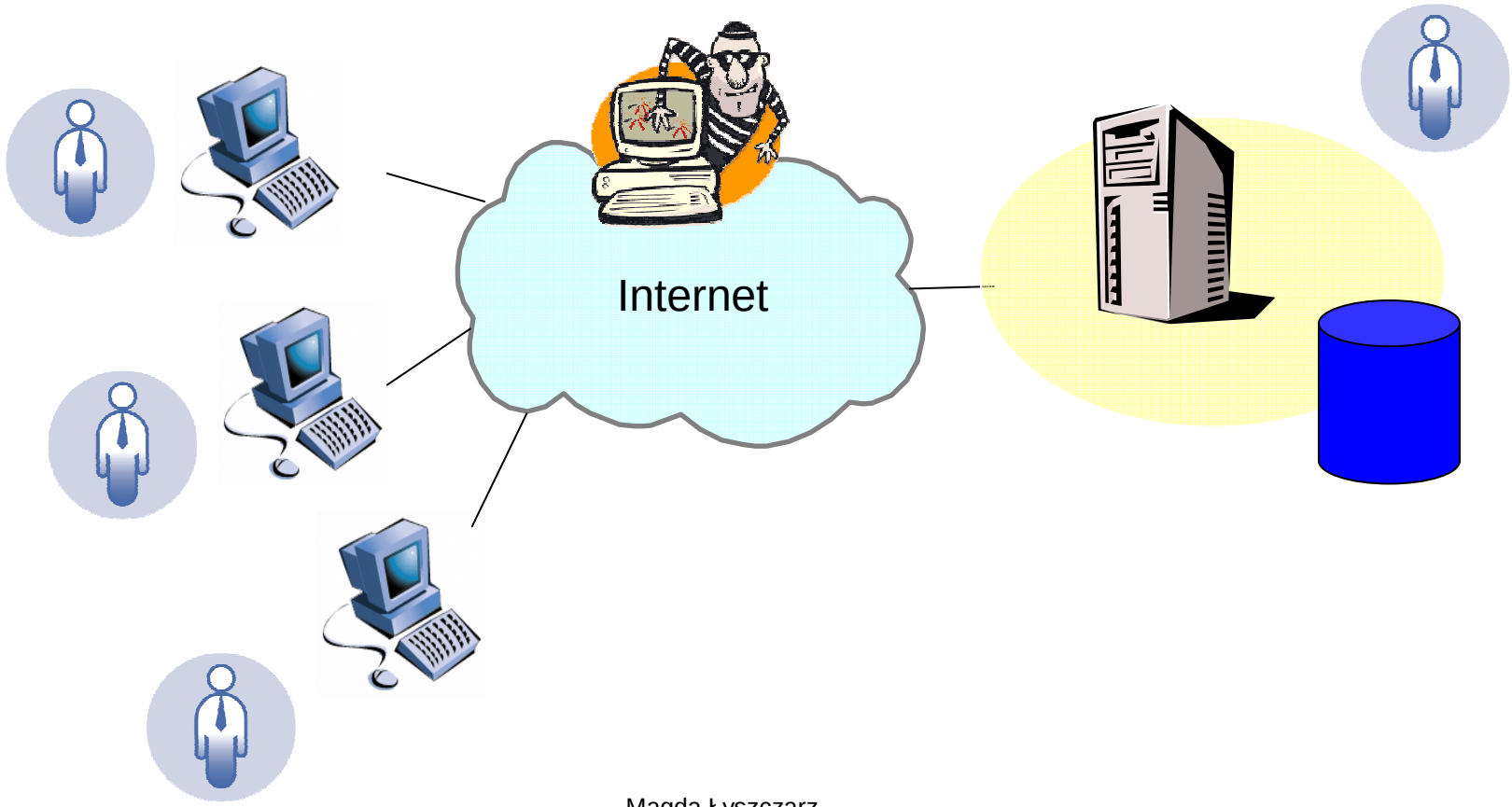
- Otrzymana wiadomość 10001100100

Obliczamy x_1: 10**0**0**1**1**0**0**1**0**0** ==> x_1=0+1+0+1+0+0=0
Obliczamy x_2: 10**0**0**1****1****0**0**1****0****0** ==> x_2=0+1+0+0+0+0=1
Obliczamy x_4: 1000**1****1****0**0100 ==> x_4=1+1+0+0=0
Obliczamy x_8: 10001100**1****0****0** ==> x_8=1+0+0+0=1
Kod nadmiarowy y: 1000
Kod nadmiarowy y': 0101
Syndrom y+y'=(1+0)(0+1)(0+0)(0+1)=1101

p: 1011=11_{DEC}

K. Tyl, Kodowanie nadmiarowe. Kod Hamminga.

Środowisko operacji elektronicznych



Protokoły kryptograficzne (4/4)

- Logowanie do aplikacji
- Jednorazowe hasło wysyłane SMSem
- Podpis cyfrowy przesyłanego wyniku badania
- Zastosowanie funkcji skrótu SHA
- Podpis cyfrowy RSA skrótu otrzymanej wiadomości

Podpis tradycyjny a podpis elektroniczny

Podpis tradycyjny

- związany nierozłącznie z dokumentem
- taki sam dla wszystkich dokumentów
- stawiany na ostatniej stronie dokumentu

Podpis elektroniczny

- przypisany jednej osobie
- niemożliwy do podrobienia
- uniemożliwiający wyparcie się go przez autora
- łatwy do weryfikacji przez osobę niezależną
- łatwy do wygenerowania

- może być składowany i przesyłany niezależnie od dokumentu
- jest funkcją dokumentu
- obejmuje cały dokument taki sam dla wszystkich dokumentów
- stawiany na ostatniej stronie dokumentu

Cel zabezpieczeń

- bezpieczne (niemal nie do złamania) szyfrowanie informacji
- jednoznaczną identyfikację nadawcy wiadomości
- zapewnienie integralności komunikatu (dokument nie może zostać zmieniony)

Cztery główne warunki podpisu cyfrowego

- uniemożliwienie podszywania się innych pod daną osobę (uwierzytelnienie osoby)
- zapewnienie wykrywalności wszelkiej zmiany w danych transakcji (integralność transakcji)
- zapewnienie niemożliwości wyparcia się podpisu przez autora
- umożliwienie weryfikacji podpisu przez osobę niezależną

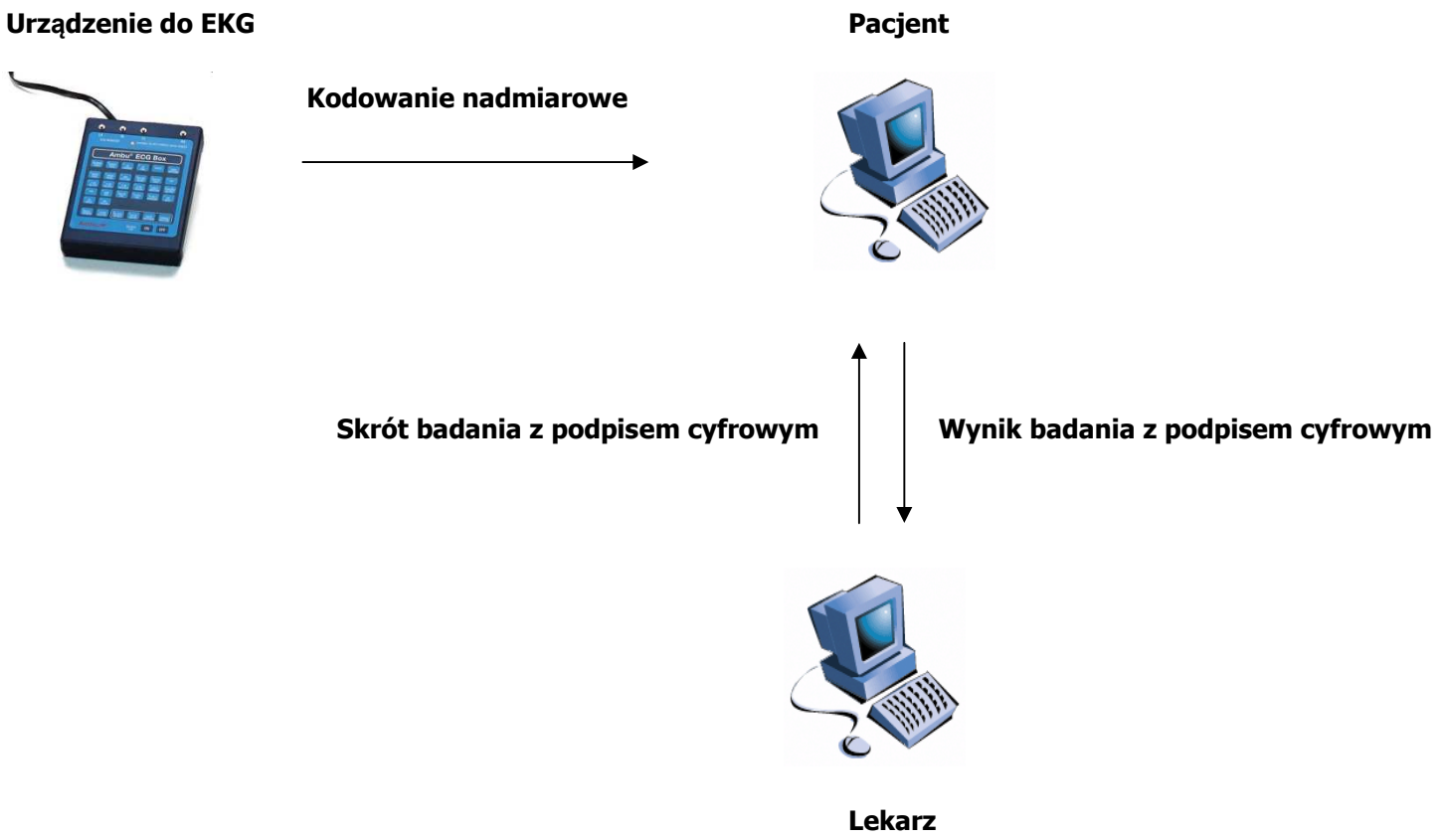
Aplikacja

Urządzenie do EKG - kodowanie wyniku badania nadmiarowo, wysłanie na komputer/komórkę pacjenta

Pacjent – loguje się do aplikacji, otrzymuje jednorazowe hasło na komórkę, badanie jest odkodowywane, podpisywane cyfrowo i wysyłane do lekarza

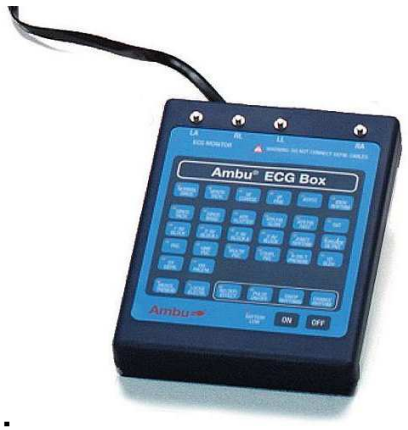
Lekarz – loguje się do aplikacji, odbiera wynik badania, wysyła do pacjenta podpisany skrót wiadomości

Architektura aplikacji



Urządzenie do EKG

1. Wykonanie badania
   - analogowy -> 2
   - cyfrowy -> 3



2. Zamiana sygnału analogowego na cyfrowy

3. Kodowanie nadmiarowe wyniku badania

4. Przesłanie wyniku badania na komputer lub telefon

Pacjent

5. Zalogowanie do aplikacji

6. Otrzymanie hasła jednorazowego

10. Wysłanie wyniku badania

7. Odbiór wyniku badania

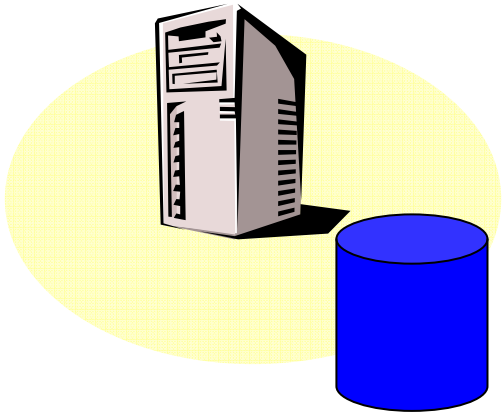
8. Odkodowanie sygnału

9. Podpis cyfrowy wyniku badania

Lekarz

11. Logowanie do aplikacji

12. Uwierzytelnienie pacjenta



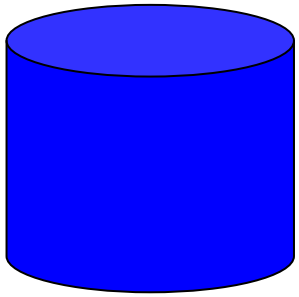
13. Odebranie wyniku badania

16. Wysłanie podpisanego skrótu wiadomości

15. Podpis cyfrowy skrótu wiadomości

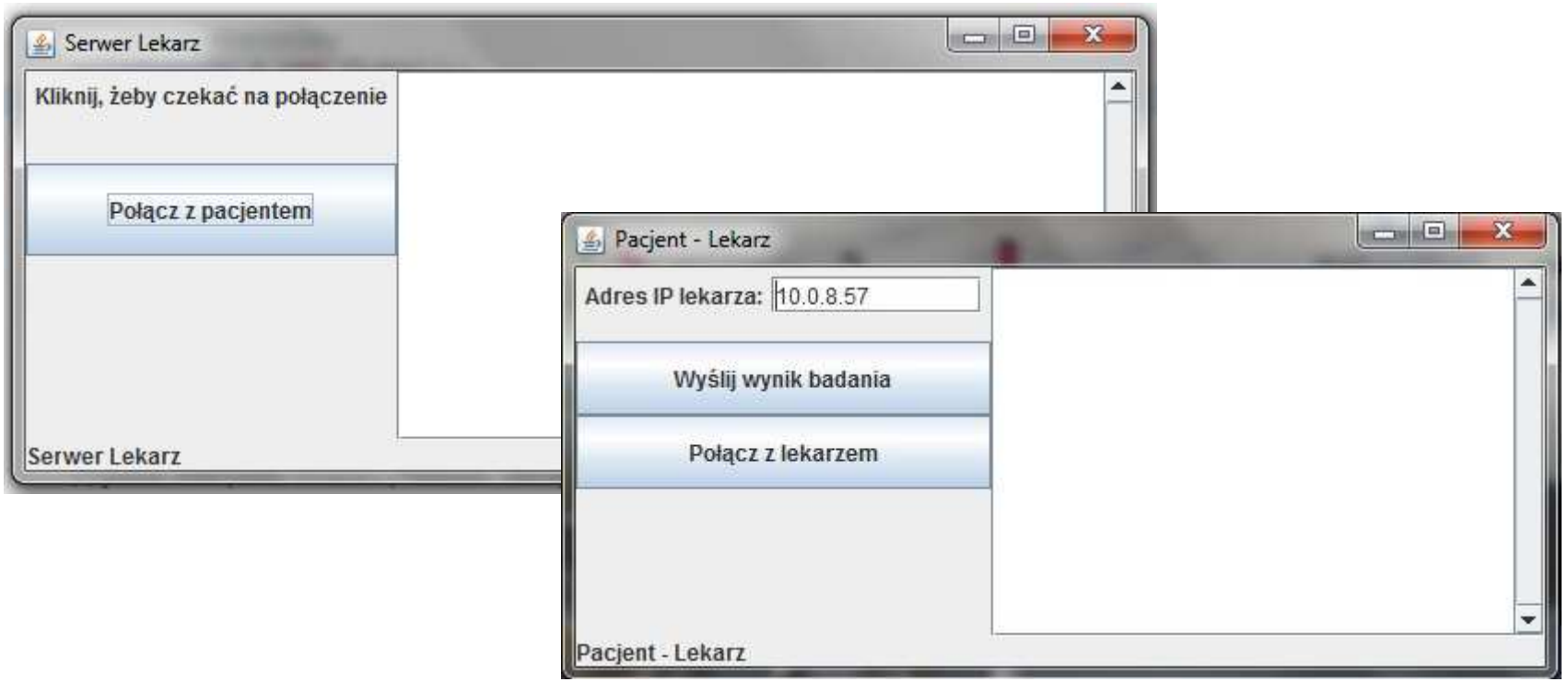
14. Wykonanie skrótu wyniku badania

Baza danych



- Zawiera dane pacjentów oraz archiwum z wynikami badania
- Zawiera login i hasło użytkowników – przetrzymuje ja w postaci zahaszowanej
- Potwierdza poprawność danych przy logowaniu – inicjuje wysłanie hasła jednorazowego do pacjenta
- Zawiera historie komunikatów wysyłanych między lekarzem a pacjentem

Wstępna wersja aplikacji



Dalsze plany

- Dopracowanie aplikacji i rozszerzenie jej o zastosowanie haseł jednorazowych
- Zaimplementowanie algorytmu kodowania nadmiarowego
- Opisanie otrzymanych wyników

Rozwój projektu

- Zwiększenie mobilności aplikacji – przeniesienie jej na telefony komórkowe
- Rozwiązanie problemu synchronizacji
- Próba odtworzenia prawdziwego przebiegu badania
- Stworzenie archiwum

Bibliografia

Pozycje literaturowe

- M. Karbowski, Podstawy kryptografii, Helion 2008
- Johannes A. Buchmann, Wprowadzenie do kryptografii, PWN 2006
- Douglas R. Stinson, Kryptografia : w teorii i w praktyce, WNT 2005
- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Kryptografia stosowana, WNT 2005

Czasopisma

- „Introducing Mobile Technologies in Support of Healthcare” w tłumaczeniu Ireneusza Wojtkowskiego

Inne

- Wykłady z przedmiotu Protokoły kryptograficzen autorstwa prof. dr hab. inż. Zbigniew Kotulski

Dziękuję za uwagę