11 Metody uwierzytelniania:

A- podmiot(strona) uwierzytelniany
B- podmiot (strona) uwierzytelniający

11.1 Hasła

A dostaje od zaufanej strony certyfikat: Cert=($Id_{A,f}$, f(wD)), gdzie f jest zadaną funkcją jednokierunkową a ‘w’- hasło

Uwierzytelnianie:

A „wpisuje” w, system oblicza f(w) i przekazuje do B

11.2 Protokół wyzwanie- odpowiedz

Zakładamy, że A i B

I) B generuje losowe wyzwanie r

II) A odpowiada i przekazuje do B wartość f(s,r), gdzie f jest zadaną funkcją jednokierunkową

III)B wykonuje to samo obliczenie i uwierzytelnia A jak wyniki zgadzają się

11.3 Uwierzytelnianie w systemie z kluczem publicznym

s-sekret strony A, S=Φ(s) wartość przekazana dla B

Wtedy powyższy protokół można identyfikować z „podpisem” strony A pod wiadomością „r”

11.4 Protokół LAMPORTA

A generuje losowe w i oblicza ciąg wartości funkcji haszującej

$h(w), h(h(w))=h^2(w),\ldots\ldots,h^k(w)=h(h^{k-1}(w))$

Niech $Cert=(Id_A, h, h^k(w))$ będzie certyfikatem strony A

Uwierzytelnianie:

Strona A przekazuje $h^{k-1}(w)$ i Cert dla B

Strona B oblicza $h(h^{k-1}(w))$ i sprawdza zgodność z wartością w certyfikacie

W kolejnych uwierzytelnieniach strona A przekazuje do B wartość h^{k-1} a strona B sprawdza czy $h(h^{k-1}(w))=h^{k-1}$

11.5 Protokół FIATA-SHAMIRA

Jest to protokół o wiedzy zerowej, w którym strona uwierzytelniana dowodzi, że zna pewną tajemnice a strona B z prawdopodobieństwem bliskim jedności przekonuje się o wiarygodności A. W czasie protokołu B nie uzyskuje, żadnej wiedzy na temat tajemnicy strony A

I) A losuje s i oblicza $y=s^2(\text{mod } n)$, które przekazuje do B wraz z certyfikatem
II) B generuje losowe r ($1<r<n$) oraz $b \in \{0,1\}$ i przesyła do A
III) A oblicza i wysyła do B wartość $t^b * r(\text{mod } n)$
IV) B sprawdza czy $(t^b * r)^2=x^b * r^2(\text{mod } n)$

(II,III,IV)-tzw. Runda

Tę rundę powtarzamy k- razy wtedy prawdopodobieństwo „fałszywego” uwierzytelniania nie przekracza 2^{-k}

Bezpieczeństwo tego protokołu Fiata- Shamira wynika stąd, że pierwiastkowanie(kwadratowe) modulo liczba złożona jest protokołem obliczeniowo trudnym. O ile nie znamy rozkładu na czynniki pierwsze.

Agitacja:

Powiedzmy, że znany jest wydajny algorytm C, który znajduje dla losowego

$y \in (Z_n^*)^Z$ wartości któregokolwiek losowego z 4 pierwiastków z

$\sqrt{y} (\mathrm{mod}\, n)$

Wykorzystując te wartość dwukrotnie otrzymamy, że jeśli $\sqrt{y} = x_1$ i $\sqrt{y} = x_2$

to $(x_1 * x_2^{-1})^2 = y * y^{-1} = 1 (\mathrm{mod}\ n)$

Zatem algorytm C pozwala efektywnie znaleźć każdy pierwiastek kwadratowy z 1(modulo n) to oznacza, że znajduje losową wartość x, spełniającą równanie $x^2 = 1 (\mathrm{mod}\ n)$.

Zatem obliczając NWD(x-1, n) z prawdopodobieństwa ≥ 0,5(jedna druga) znajdziemy nietrywialny dzielnik pierwszej liczby n.

To wynika z faktu, że jeśli x=1(mod p) i x=-1(mod q)

lub x=-1(mod p) i x=1(mod q)

to NWD (x-1, n)=p

lub NWD(x-1,n)=q