1. ker...: Przeciwnik zna użyty kryptosystem, nie zna natomiast zastosowanych kluczy. Określa ogólne warunki bezpieczeństwa kryptosystemu.
2. Szyfr Vigenere'a: W szyfrach podstawieniowych każda litera tekstu jawnego zamieniana jest na tylko jedną literę szyfrogramu. Kryptosytemy o tej własności nazywane są monoalfabetycznymi. Przedstawimy teraz szyfr Vigenere'a (dyplomata francuski Blaise de Vigenere żył w latach 1523-1596), w którym poszczególne litery tekstu jawnego mogą być przekształcone na różne litery alfabetu szyfrogramu. Określony przez niego kryptosystem należy do kategorii polialfabetycznych. Niech $m \geq 2$ będzie ustaloną liczbą naturalną.
3. vernam: identycznej długości, co tekst jawny. klucz jest użyty tylko raz.
4. shannon: potwierdzeniem teorii shannona jest szyfr vernama. elementy klucza muszą być losowe.
5. DES: 64 bit klucz, 56 efektywny klucz (8 bitów parzystości), symetryczny, blokowy, 16 rund, 64 bitów na blok, 16 podkluczy 48 bitowych
6. AES: klucz 128 bitów lub 192 lub 256 bitów, blok 128 bit, 8 rund
7. skróty: Jednokierunkowa funkcja skrótu jest przekształceniem, które z wiadomości o dowolnej długości generuje krótką wartość (skrót), unikalny i charakterystyczny dla tej wiadomości. Podstawowymi cechami, które muszą spełniać funkcje skrótu jest wrażliwość na zmiany w oryginalnym tekście (jeden zmieniony bit wiadomości powinien spowodować zmianę wszystkich bitów skrótu) oraz małe prawdopodobieństwo kolizji (prawdopodobieństwo istnienia dwóch wiadomości o identycznych skrótach musi być bardzo małe). Funkcja skrótu musi być także nieodwracalna, to znaczy nie może się dać obliczyć oryginalnego tekstu wiadomości na podstawie jej skrótu.
Warunki: - dla danego M łatwo jest obliczyć h(M); - znalezienie M, dla którego znamy h(M) jest obliczeniowo nie możliwe (jednokierunkowość); - dla danej wiadomości M jest obliczeniowo niemożliwe znalezienie takiej wiadomości M' M, że:
h(M')=h(M); - jest obliczeniowo nie możliwe znalezienie dwóch dowolnych różnych wiadomości M i M', że:
h(M')=h(M); - współcześnie bezpieczne długości skrótów: 128 bitów, 160 bitów;
8. funkcje skrótu snerfu - 128 bit lub 256, n-hash - 128 bit., md2, md4, md5 - 128 bit., sha-1 - 160 bit., haval - 128, 160, 192, 224 bit.
9. kryptosystem klucza publicznego: Scharakteryzuj kryptosystem asymetryczny. Nadawca i odbiorca używają różnych kluczy. Podstawą algorytmu asymetr jest jawność klucza. Używa się 2 lub więcej kluczy i występuj one w parach. Jeden do szyfr drugi do deszyfr. Opublikowanie jednego z nich nie zdradza drugiego. Zwykle jeden z nich np. klucz szyfrujący jest ogólnie dostępny i nosi nazwę klucza publicznego. Drugi jest kluczem prywatnym i jest trzymany w tajemnicy. Podaj przykłady kryptosystemów klucza publicznego. Na jakich problemach bazują te kryptosystemy?
Kluczem publicznym nazywamy jeden z pary kluczy. Jest on powszechnie dostępny, może to być klucz szyfrujacy lub deszyfrujący zależnie od zastosowania. Jego odpowiednikiem w parze jest klucz prywatny (niejawny)
Gdy kluczem publicznym jest klucz szyfrujący wówczas każdy posiadający ten klucz szyfruje nim informację i przekazuje odbiorcy. Odbiorca posługując się swoim kluczem prywatnym jest w stanie odczytać informację.
Z odwrotną sytuacja mamy doczynienia w przypadku podpisów elektronicznych. Klucz szyfrujący jest kluczem prywatnym i tylko nadawca może zaszyfrować swój podpis. Odbiorca posługujący się kluczem publicznym (deszyfrującym) może odczytac podpis każdego nadawcy.
10. RSA Na czym opiera się bezpieczeństwo RSA? Czego poszukuje kryptoanalityk? Jakie wielkości parametru n uznaje się za bezpieczne? Bezpieczeństwo RSA opiera się na tym, że aby złamać szyfr należałoby rozłożyć n na czynniki pierwsze. Problem rozkładu liczby na czynniki pierwsze jest problemem klasy NP., ale nie wiadomo, czy jest to problem NP-zupełny, co świadczyłoby o jego trudności. Z drugiej jednak strony najlepsze obecnie znane algorytmy rozkładające liczby na czynniki pierwsze wymagają dość dużych czasów obliczeń. Powoduje to, że tylko dla stosunkowo niewielkich wartości n metoda ta może być stosowana. Klucz 1024 bity zalecany.
11. poufność Prywatność i poufność: utrzymywanie informacji w tajemnicy dla wszystkich poza uprawnionymi
12. integralność zapewnienie niezmienności informacji w nieuprawniony lub nieznany sposób
13. uwierzytelnianie Uwierzytelnienie lub identyfikacja strony: potwierdzenie tożsamości strony (osoby, terminala komputerowego karty kredytowej, itd.) Uwierzytelnienie wiadomości: potwierdzenie źródła informacji; uwierzytelnienie oryginalności danych
14. podpis cyfrowy 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 transmitowany niezależnie od dokumentu, Jest funkcją dokumentu, Obejmuje cały dokument
15. d-h ma na celu ustalenie wspólnej, tajnej liczby między stronami. jego bezpieczeństwo oparte jest na trudnym obliczeniowo problemie logarytmu dyskretnego