ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1995

Seria: INFORMATYKA z. 28 Nr kol. 1270

Janusz STOKŁOSA

ZABEZPIECZENIA KRYPTOGRAFICZNE W SIECIACH KOMPUTEROWYCH

Streszczenie. W artykule dokonano przeglądu mechanizmów kryptograficznych, stanowiących podstawę do projektowania złożonych zabezpieczeń kryptograficznych. Za kryterium podziału mechanizmów przyjęto używanie lub nieużywanie klucza kryptograficznego. Szczególna uwagę zwrócono na szyfry symetryczne i asymetryczne, funkcje haszowe, protokoły uwierzytelniania i protokoły wymiany kluczy kryptograficznych. Mechanizmy te tworzą warstwową architekturę zabezpieczeń kryptograficznych.

SECURITY TECHNIQUES IN COMPUTER NETWORKS

Summary. In the paper a survey of cryptographic mechanisms is presented. They are intended to be basic to design complex cryptographic mechanisms. Symmetric and asymmetric ciphers, hash functions, authentication protocols and protocols for the exchange of cryptographic keys are of special interest here. They form a layered architecture of cryptographic protection in computer networks.

TECHNIQUES DE SECURITE DANS LES RESEAUX DES ORDINATEURS

Résumé. Dans l'article on a presenté des méchanismes cryptographiques utilisés dans les réseaux des ordinateurs. On a souligné l'importance de chiffrement symmétrique et asymmétrique, de protocols d'authentification et de protocols de gestion de clés. Tous ces méchanismes forment l'architecture de couche de protection cryptographique.

Pracę wykonano na Politechnice Poznańskiej w ramach badań statutowych nr 45/268/94/DS.

1. Wprowadzenie

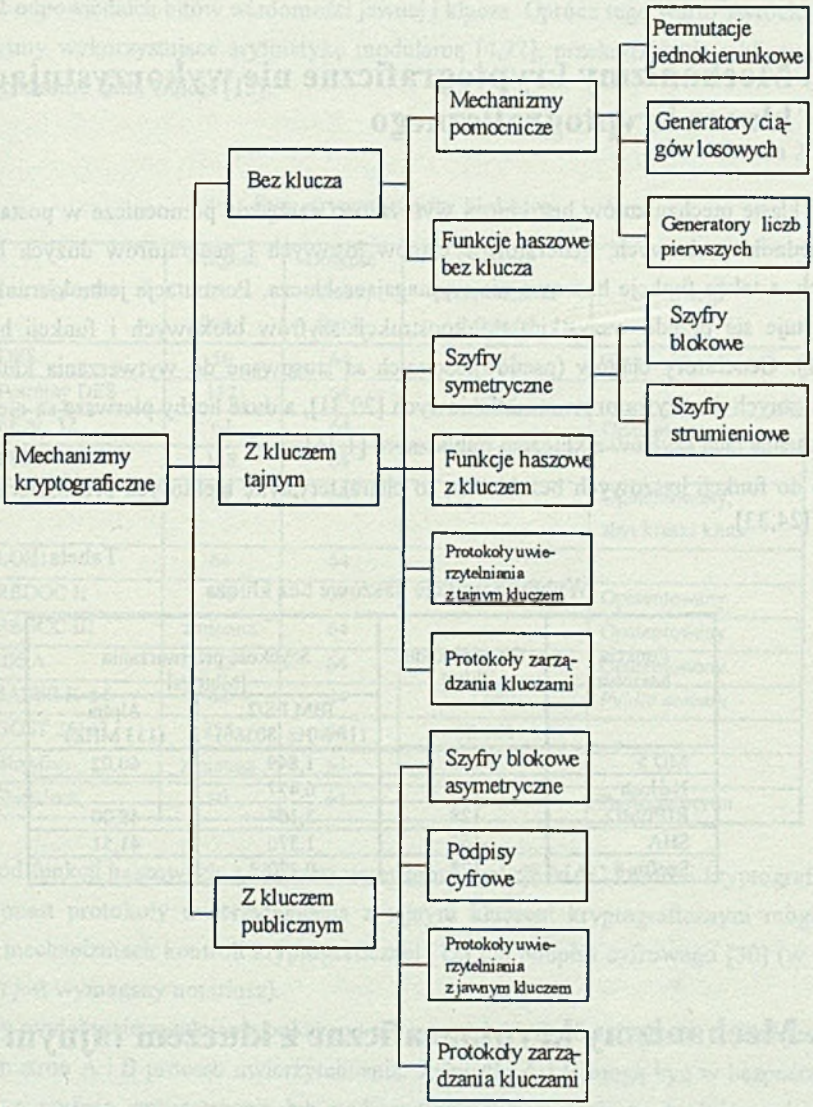
Norma [8] (por. także [23]) określa architekturę zabezpieczeń Modelu Odniesienia ISO OSI. Wyspecyfikowano w niej zagrożenia systemów otwartych w postaci czynników pasywnych, aktywnych i maskarady. Wymienionym zagrożeniom można przeciwdziałać korzystając z usług uwierzytelniania, kontroli dostępu, poufności, integralności i nieodrzucania. Usługi te realizuje się za pomocą mechanizmów szyfrowania, podpisu cyfrowego, kontroli dostępu, integralności danych, uwierzytelniania, wypełniania ruchu, notaryzacji oraz sterowania wyborem drogi. Co do kryptografii, to stanowi ona podstawę licznych usług i mechanizmów zabezpieczających. Odnosi się to do wszystkich warstw modelu OSI z wyjątkiem warstwy sesji, w której nie są realizowane żadne usługi zabezpieczeń.

Od 1986 roku Komisja Wspólnot Europejskich sponsorowała przedsięwzięcie pt. "Mechanizmy zabezpieczeń w sieciach komputerowych" [17]. W trakcie realizacji rozszerzono je tak, aby pokrywało zagadnienia związane z otwartym przetwarzaniem rozproszonym (ODP - *Open Distributed Processing*). W rezultacie powstał projekt zaprezentowany w [19,20]. Wszechstronny System Zintegrowanego Bezpieczeństwa (CISS - *Comprehensive Integrated Security System*) będący końcowym rezultatem projektu wymaga wprowadzenia usług w zakresie bezpieczeństwa przy przesyłaniu danych i zdalnym dostępie użytkownika końcowego do komputera. CISS [18] składa się z czterech warstw funkcjonalnych: najniższą zajmują elementarne moduły matematyczne i segmenty (parametry) Bazy Informacji Zarządzania Bezpieczeństwem (SMIB - *Security Management Information Base*), w warstwie wyższej są mechanizmy indywidualnych zabezpieczeń, w kolejnej warstwie umieszczono protokoły zabezpieczeń, a w warstwie najwyższej znalazły się moduły nadzorujące, koordynujące i zarządzające systemem zabezpieczeń. Mechanizmy zdefiniowane w warstwie wyższej korzystają z modułów warstwy niższej. CISS zaimplementowano w całości. Komponenty składające się na warstwę najniższą i tworzące tzw. uogólnioną bibliotekę zabezpieczeń obejmują: generator dużych liczb losowych, generator i tester dużych liczb pierwszych, 16-, 32-, 64-, 128- i 160-bitową funkcję haszową MD5, algorytmy symetryczne DES i FEAL, algorytmy asymetryczne RSA i ElGamala, a także schemat (wiedzy zerowej) uwierzytelniania Fiata-Shamira.

Te i inne przedsięwzięcia w zakresie ochrony danych (por. np. [14,25]) w sieciach komputerowych i systemach rozproszonych wykorzystują dokonania kryptograficzne.

2. Klasyfikacja mechanizmów kryptograficznych

Podział mechanizmów kryptograficznych przedstawiono na rysunku 1. Jako główne kryterium podziału przyjęto stosowanie bądź niestosowanie klucza kryptograficznego. Przy takim



Rys. 1. Klasyfikacja mechanizmów kryptograficznych
Fig. 1. Classification of cryptographic mechanisms

podejściu wyróżnia się mechanizmy bez klucza kryptograficznego, z kluczem tajnym i z kluczem publicznym. Każda z tych klas mechanizmów kryptograficznych zawiera w sobie kilka podklas. Mechanizmy w poszczególnych podklasach służą bądź to do projektowania algorytmów kryptograficznych lub stanowią narzędzia pomocnicze, bądź do realizacji wybranego typu systemu kryptograficznego (symetryczny lub asymetryczny).

3. Mechanizmy kryptograficzne nie wykorzystujące klucza kryptograficznego

W klasie mechanizmów bez klucza wyróżniono narzędzia pomocnicze w postaci permutacji jednokierunkowych, generatorów ciągów losowych i generatorów dużych liczb pierwszych, a także funkcje haszowe nie wymagające klucza. Permutacje jednokierunkowe wykorzystuje się przede wszystkim do konstrukcji szyfrów blokowych i funkcji haszowych [22,31]. Generatory ciągów (pseudo)losowych są stosowane do wytwarzania kluczy kryptograficznych dla szyfratorów strumieniowych [29,31], a duże liczby pierwsze są niezbędne w implementacjach szyfrów z kluczem publicznym [1,16].

Co do funkcji haszowych bez klucza, to charakterystykę niektórych przedstawiono w tabeli 1 [24,33].

Tabela 1

Wybrane funkcje haszowe bez klucza

Funkcja haszowa	Długość kodu [bity]	Szybkość przetwarzania [Mbity/s]	
		IBM PS/2 (16 MHz 80386)	Alpha (133 MHZ)
MD 5	128	1,849	60,02
N-Hash	128	0,477	
RIPEMD	128	3,104	48,00
SHA	160	1,370	41,51
Snefru-8	128	0,270	

4. Mechanizmy kryptograficzne z kluczem tajnym

Do mechanizmów kryptograficznych z kluczem zaliczono na rysunku 1 szyfry blokowe i strumieniowe, funkcje haszowe z kluczem oraz protokoły uwierzytelniania z tajnym kluczem kryptograficznym. Charakterystykę wybranych szyfrów blokowych zamieszczono w

tabeli 2. Dane co do szybkości przetwarzania zaczerpnięto z [27]. Są to wyniki eksperymentów przeprowadzonych na komputerze DEC 3000/400 "Sandpiper" z procesorem Alpha taktowanym częstotliwością 133 MHz i wyposażonym w pamięć notatnikową 2x8 KB (podstawową) i 512 KB (wtórną).

Szyfry strumieniowe od dawna budzą zainteresowanie implementatorów [2,4,29]. W większości rozwązań są to przekształcenia dokonywane w $GF(2^p)$, polegające na dodawaniu modulo 2 odpowiednich bitów wiadomości jawnej i klucza. Oprócz tego warto zwrócić uwagę na algorytmy wykorzystujące arytmetykę modularną [4,22], przekształcenia tablicowe [28], czy tzw. rzekome ciała Galois [15].

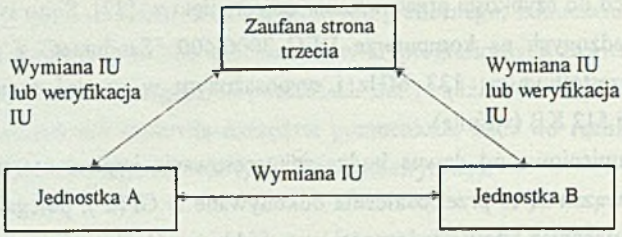
Tabela 2

Symetryczne szyfry blokowe

Algorytm	Długość klucza [bity]	Długość bloku [bity]	Szybkość przetwarzania [Mbity/s]	Uwagi
DES	56	64	1.855	Zbyt krótki klucz
Potrójny DES	112	64	1.855	
FEAL 32	64	64		Opatentowany
FEAL NX	128	64		
Khufu	64	64		Opatentowany, zbyt krótki klucz
LOKI	64	64		
REDOC II	140	70		Opatentowany
REDOC III	zmienna	64		Opatentowany
IDEA	128	64		Opatentowany
SAFER K-64	64	64	7.680	*Public domain*
GOST 28147	256	64	2.909	
Blowfish	zmienna	64		
Skip-Jack	80	64		Tajny algorytm

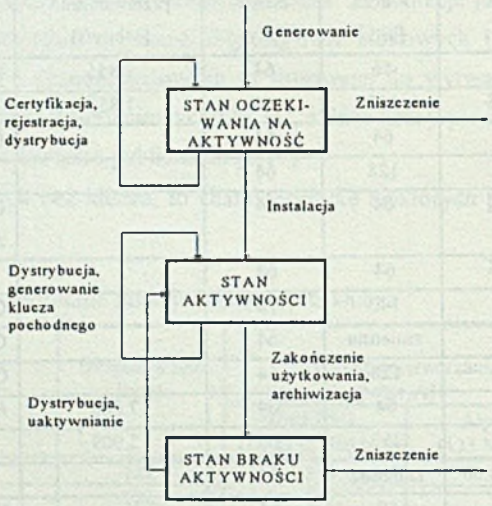
Spośród funkcji haszowych z kluczem wymieńmy funkcję MAC kontroli kryptograficznej [9]. Natomiast protokoły uwierzytelniania z tajnym kluczem kryptograficznym mogą być oparte na mechanizmach kontroli kryptograficznej [12] lub podpisu cyfrowego [30] (w takim przypadku jest wymagany notariusz).

Ogólny model uwierzytelniania pokazano na rysunku 2. Zaufana strona trzecia jest powiernikiem stron A i B procesu uwierzytelniania. Jednostki A i B mogą być w bezpośrednim kontakcie z zaufaną stroną trzecią lub wykorzystywać informacje pochodzące od strony trzeciej w trakcie wymiany lub/i weryfikacji informacji uwierzytelniającej (IU). Protokoły uwierzytelniania z wykorzystaniem klucza tajnego opisano w [10].



Rys.2. Model uwierzytelniania
Fig.2. Authentication model

Zarządzania kluczami kryptograficznymi można dokonywać stosując protokoły wykorzystujące szyfry symetryczne [13] i asymetryczne [3]. Obejmuje ono generowanie, instalację i archiwizację kluczy. Diagram stanów objaśniający cykl życia klucza ilustruje rysunek 3. W procesie zarządzania korzysta się z protokołów uzgadniania i przesyłania kluczy. Wykorzysty-



Rys. 3. Diagram stanów cyklu życia klucza kryptograficznego
Fig.3. State diagram of cryptographic key life-cycle

wane mechanizmy, to schemat Diffie-Hellmana [6], ElGamala [7], Matsumoto-Takashima-Imai [21]. W procesie dystrybucji pomocny jest urząd certyfikujący (ang. *certification authority*), którego istnienie jest nieodzowne przy tego typu działaniach. Klasa protokołów wymiany kluczy kryptograficznych w systemach z prywatnym kluczem obejmuje m.in. [3,31,32] protokół Cerbera, szerokogębnej żaby, Yahaloma, Otway a-Rees a, Needhama-Schroedera.

5. Mechanizmy kryptograficzne z kluczem publicznym

Największym zainteresowaniem w tej grupie cieszą się szyfr RSA i szyfr ElGamala (por. [1]) - obydwa są szyframi wykładniczymi. Ich moc zasadza się na dużej złożoności obliczeniowej logarytmowania dyskretnego i dużej złożoności obliczeniowej rozkładu liczb złożonych na czynniki pierwsze. Co do faktoryzacji liczb złożonych, to eksperymenty wskazują, że jeśli używać liczb pierwszych ponad 100-cyfrowych, a najlepiej około 150-cyfrowych, to prawdopodobieństwo faktoryzacji liczby złożonej około 300-cyfrowej, a w konsekwencji złamania szyfru, np. RSA, jest znikomo małe. Wadą szyfrów wykładniczych jest niewielka szybkość przetwarzania danych, co zilustrowano w tabeli 3 na przykładzie dostępnych na rynku układów scalonych realizujących szyfr RSA [1,32].

Oprócz szyfrów wykładniczych pod uwagę bierze się także szyfry plecakowe. Pomimo wykazania, iż addytywne szyfry plecakowe można złamać w czasie wielomianowym, tego typu algorytmy budzą wciąż żywe zainteresowanie badaczy [5].

Szyfry kryptografii asymetrycznej są szczególnie wygodne w realizacji podpisów cyfrowych. Podpisem cyfrowym każdej wiadomości jest jej postać zaszyfrowana za pomocą klucza tajnego. Weryfikacja podpisu następuje po jego zaszyfrowaniu kluczem jawnym [1,26,31,32].

Do uwierzytelniania stosuje się nie tylko podpisy cyfrowe. Wchodzą tu także w grę protokoły uwierzytelniania z jawnym (publicznym) kluczem [30,31].

Tabela 3

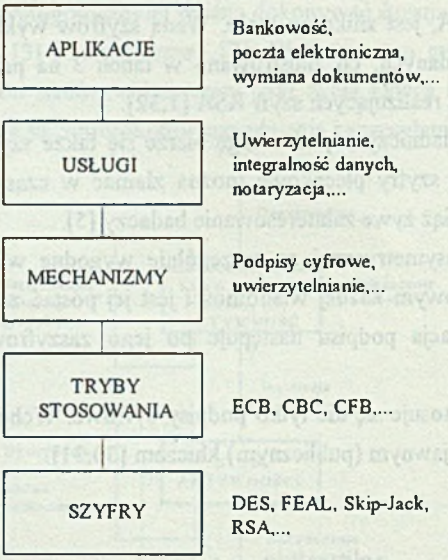
Układy scalone implementujące RSA

Producent	Częstotliwość zegara [MHz]	Pasmo przenoszenia 512-bitowych bloków [10^6 bloków/s]	Liczba okresów zegara niezbędnych do zaszyfrowania 512-bitowego bloku [x10^6]
AT&T	15	19	0,4
British Telecom	10	5,1	1
Business Sim. Ltd.	5	3,8	0,67
CNET	25	5,3	2,3
Cryptech	14	17	0,4
Cylink	16	6,8	1,2
Pijnenburg	25	50	0,256
Sandia	8	10	0,4

Na rysunku 3 przedstawiono diagram stanów cyklu życia klucza kryptograficznego, wskazując jednocześnie protokoły wymiany, do realizacji których używa się kluczy tajnych. Znane są także tego typu protokoły wykorzystujące klucze publiczne [3,11].

6. Uwagi końcowe

Algorytmy kryptograficzne stanowią podstawę licznych zastosowań. Są wykorzystywane w różnych trybach pracy, używa się ich do projektowania mechanizmów integralności, usług i aplikacji. Architekturę zabezpieczeń kryptograficznych pokazano na rysunku 4. Wars twę dolną tworzą szyfry. Każda wyższa warstwa korzysta z obiektów dostępnych w warstwie niższej.



Rys.4. Architektura zabezpieczeń kryptograficznych
Fig.4. Architecture of cryptographic security

LITERATURA

[1] Beth Th., Frisch M., Simmons G.J. (eds): Public-Key Cryptography: State of the Art and Future Directions. LNCS 578, Springer, Berlin 1992.
[2] Bloecher U., Dichtl M.: A fast software stream cipher. Andreson R. (Ed.), Fast Software Encryption. LNCS 809, Springer, Berlin 1994, 41-44.
[3] Burrows M., Abadi M., Needham R.: A logic of authentication. ACM Transactions on Computer Systems, Vol.8, No.1, 1990, 18-36.

[4] Chambers W.G.: Two stream ciphers. Andreson R. (Ed.), Fast Software Encryption. LNCS 809, Springer, Berlin, 1994, 51-55.
[5] Chor B.-Z.: Two Issues in Public Key Cryptography. RSA Bit Security and a New Knapsack Type System. The MIT Press, Cambridge, MA, 1986.
[6] Diffie W., Hellman M.E.: New directions in cryptography. IEEE Transactions on Information Theory, Vol.IT-22, No. 6, 1976, 644-654.
[7] ElGamal T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, Vol.IT-31, No.7, 1985, 469-472.
[8] ISO 7498-2:1989 Information processing systems - Open Systems Interconnection - Basic Reference Model. Part 2: Security Architecture .
[9] ISO/IEC 9797: 1989 Data cryptographic techniques - Data integrity mechanisms using a cryptographic check function employing a block cipher algorithm.
[10] ISO/IEC DIS 9798-2: 1994 Information technology - Security techniques - Entity authentication - Part 2: Entity authentication using symmetric techniques.
[11] ISO/IEC DIS 9798-3: 1994 Information technology - Security techniques - Entity authentication - Part 3: Entity authentication using a public key algorithm.
[12] ISO/IEC DIS 9798-4: 1994 Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function.
[13] ISO/IEC 2nd CD 11770-2: 1993 Information technology - Security techniques - Key Management - Part 2: Key Maanagement Mechanisms Using Symmetric Techniques.
[14] Kirstein P.T., Williams P.: Piloting authentication and security services within OSI applications for RTD information (PASSWORD). Computer Networks and ISDN Systems, Vol.25, No.4-5, 1992, 483-489.
[15] Kościelny Cz.: A method of constructing fast, easily implemented yet secure stream-ciphers. Preprinty nr 37/94, Wydawnictwo Politechniki Wrocławskiej, Wrocław 1994.
[16] Kranakis E.: Primality and Cryptography. Taubner-Stuttgart, Wiley-Chichester 1986.
[17] Muftic S.: Security mechanisms for computer networks (A program of the CEC COST-11 Ter Project). Computer Networks and ISDN Systems, Vol.12, No.5, 1986, 339-344.
[18] Muftic S.: Implementation of the Comprehensive Integrated Security System for computer networks. Computer Networks and ISDN Systems, Vol.25, No.4-5, 1992, 469-475.
[19] Muftic S.: Security architecture for ODP systems. Final results of the CEC COST-11 Ter "Security" Project. Computer Networks and ISDN Systems, Vol.26, No.11, 1994, 1343-1349.
[20] Muftic et al.: Security Architecture for Open Distributed Systems. J. Wiley, Chichester 1993.
[21] Mutsamoto T., Takashima Y., Imai H.: On seeking smart public-key distribution systems. Transactions of the IECE of Japan, Vol.E69, No.2, 1986, 99-106.
[22] Pieprzyk J., Sadeghiyan B.: Design of hashing algorithms. LNCS 756, Springer, Berlin 1993.
[23] PN-92/T-20001/02 Systemy przetwarzania informacji. Współdziałanie systemów otwartych (OSI). Podstawowy Model Odniesienia. Architektura zabezpieczeń.
[24] Preneel B.: Design principle for dedicated hash functions. Andreson R. (Ed.), Fast Software Encryption. LNCS 809, Springer Berlin, 1994, 71-82.
[25] Purser M.: COSINE Sub-Project P8: security services. Computer Networks and ISDN Systems, Vol.25, No.4-5, 1992, 476-482.
[26] Robling Denning D.: Kryptografia i ochrona danych. WNT, Warszawa 1992.

[27] Roe M.: Performance of symmetric ciphers and one-way hash functions. Andreson R. (Ed.), Fast Software Encryption. LNCS 809, Springer, Berlin, 1994, 83-89.
[28] Rogaway Ph., Coppersmith D.: A software-optimized encryption algorithm. Andreson R. (Ed.), Fast Software Encryption. LNCS 809, Springer, Berlin 1994, 56-63.
[29] Rueppel R.A.: Analysis and Design of Stream Ciphers. Springer, Berlin 1986.
[30] Stokłosa J.: Kryptograficzne metody ochrony danych. Wydawnictwo Politechniki Poznańskiej, Poznań 1992.
[31] Stokłosa J.: Algorytmy kryptograficzne. OWN PAN, Poznań 1994.
[32] Stokłosa J.: Kryptograficzna ochrona danych w systemach komputerowych. Wydawnictwo Nakom, Poznań 1994.
[33] Stokłosa J.: Kryptograficzna ochrona danych w praktyce informatycznej. Konferencja "Informatyka na wyższych uczelniach dla gospodarki narodowej", Gdańsk 17-19 listopada 1994, t. II, 161-167.

Rencenzent: Dr inż. Ryszard Maceluch

Wpłynęło do Redakcji 15 listopada 1994 r.

Abstract

In the paper a security architecture of cryptographic mechanisms is presented. Section 1 gives motivations for such a treatment of cryptographic mechanisms. In Section 2, Figure 1 presents a classification of cryptographic mechanisms. Mechanisms without cryptographic key are described in Section 3. The special interest is mentioned on hash functions without key. Table 1 presents chosen hash functions, indicates length of their code and speed of processing. Section 4 deals with cryptographic mechanisms using cryptographic key, i.e. symmetric block ciphers (Table 2), stream ciphers, hash function using keys, authentication protocols and key management protocols. In Section 5 cryptographic mechanisms with public key are discussed: RSA and ElGamal ciphers, knapsack ciphers, digital signatures, authentication protocols and key management protocols. Section 6 summarizes the discussion giving a layered architecture of cryptographic mechanisms (Figure 4).