Asymetrické kryptografické schéma

asymmetric encryption scheme

Klíčově závislé kryptografické schéma, které není symetrické. Asymetrické schéma obecně používá několik klíčů, které dělíme na *veřejné* a *privátní*. Ve většině případů se dnes setkáme se schématy používajícími právě jeden veřejný a právě jeden privátní klíč. Veřejné a privátní klíče, které společně tvoří danou *instanci* tohoto schématu, nazýváme *klíčový pár*. V praxi se tato schémata nejčastěji používají tak, že privátní klíč zná jen jeden konkrétní subjekt, přičemž všechny subjekty využívající danou instanci znají hodnotu veřejného klíče.

Bezkolizní funkce

collision-resistant function

Funkci f: $X \rightarrow Y$, pro níž je výpočetně neschůdné najít dvě různé hodnoty $x_{1,2} \in X$ takové, že $f(x_1) = f(x_2)$, nazveme bezkolizní.

Certifikát veřejného klíče

public key certificate

Datová zpráva, která nepopiratelným způsobem spojuje konkrétní identitu subjektu s konkrétní hodnotou veřejného klíče. Vydáváním a správou certifikátů v daném informačním systému se zabývá zejména komponenta označovaná jako *certifikační autorita*, včetně jejích subkomponent.

Digitální podpis

digital signature

V praxi se někdy ne zcela správně tento termín používá jako synonymum pro termín *podpisové schéma*. Korektnější definice říká, že digitálním podpisem nazýváme informaci, která je k podepisované zprávě připojena podpisovým schématem k tomu, aby toto schéma mohlo plnit svůj účel. Ve většině podpisových schémat používaných v současné době má informace nesoucí digitální podpis podobu samostatné binární datové zprávy, jejíž délka je v rámci konkrétní instance daného schématu pevná. Taková schémata označujeme jako *podpisová schémata s dodatkem*.

Elektronický podpis

electronic signature

Tento pojem je ve většině zemí upraven platným zákonem, nařízením či standardem. V České republice tuto úpravu provádí zákon č. 227/2000 Sb. o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění zákona č. 226/2002 Sb. S tímto zákonem ještě úzce souvisí vyhláška ÚOOÚ č. 366/2001 Sb. a nařízení vlády č. 304/2001 Sb. ze dne 25.července 2001, kterým se provádí zákon č. 227/2000 Sb.

Oblast elektronického podpisu není totožná s oblastí podpisových schémat. Proto je vhodné pojmy elektronický podpis a digitální podpis odlišovat. Obecně platí, že podpisová schémata jsou v současné době z bezpečnostního a praktického hlediska jediným vhodným kandidátem na realizaci elektronického podepisování dle výše citovaných právních norem.

Funkce (zobrazení)

function (mapping)

Funkcí f z množiny vzorů X do množiny obrazů Y, kde X a Y jsou neprázdné, nazveme pravidlo, které každému prvku (vzoru) x, $x \in X$, jednoznačně přiřadí právě jeden prvek (obraz) y, $y \in Y$. Píšeme $y = f(x)$ a také f: $X \rightarrow Y$. Poznamenejme, že zatímco v běžné technické praxi pracujeme s funkcemi, jejichž množiny vzorů (a často i obrazů) odpovídají množině reálných čísel R, v kryptografii tomu tak není. Proto je nutné věnovat tomuto aspektu jistou pozornost. Funkci, která každému jejímu obrazu y, $y \in Y$, přiřadí x, $x \in X$, takové, že $f(x) = y$, nazveme *funkcí inverzní* k f a značíme ji f^{-1}. *Parciálně inverzní* funkce g k funkci f je funkce, která je k f inverzní pouze na určité podmnožině množiny obrazů. Poznamenejme, že podaná definice f^{-1} je mírně upravena pro specifické potřeby kryptografie.

Hašovací funkce

hash function

Funkci h: $M \rightarrow Y$, kde $M = \{0,1\}^*$ je vstupní množina binárních zpráv libovolné délky a $Y = \{0,1\}^b$ je množina výstupních hodnot pevné délky b, nazýváme hašovací funkcí. Výsledek hašovací funkce $y = h(m)$ nazýváme *hašový kód* zprávy m. Hašovací funkce používané v běžných kryptografických schématech musí splňovat následující podmínky: popis funkce h je veřejný a neobsahuje žádné tajné prvky (klíče), h je *jednosměrná* a *bezkolizní*. Poznamenejme, že $|M| >> |Y|$, proto musí nutně existovat dvojice různých zpráv (m_1, m_2) takových, že $h(m_1) = h(m_2)$. Vlastnost bezkoliznosti však zaručuje, že útočník není schopen žádnou takovou dvojici nalézt.

V současné době se používají zejména funkce MD5 (od ní se upouští díky určitým náznakům slabin), SHA-1 a RIPEMD160. Zcela novými jsou standardy SHA-256, SHA-384 a SHA-512, které mají postupně doplňovat a nahrazovat SHA-1.

Jednosměrná (jednocestná) funkce

one-way function

Funkci f: $X \rightarrow Y$ nazveme jednosměrnou, když pro každé $x \in X$ je výpočetně snadné spočítat hodnotu $y = f(x)$, ale pro náhodně zvolené $y \in Y$ je výpočetně neschůdné najít $x \in X$ tak, aby platilo $f(x) = y$.

Jednosměrná (jednocestná) funkce s padacími vrátky

trapdoor one-way function

f_k: $X \rightarrow Y$ nazveme jednosměrnou funkcí s padacími vrátky (k), když f_k je jednosměrná s takovou vlastností, že při znalosti určité dodatečné informace (k) je pro každý obraz $y \in Y$ výpočetně snadné najít $x \in X$ takové, že $f_k(x) = y$, tedy $x = f_k^{-1}(y)$. Takové funkce se využívají zejména v asymetrických kryptografických schématech, kde v roli k vystupuje *privátní klíč* nebo jeho derivát.

Klíč
key

Speciální informace, kterou je ve většině kryptografických schémat nutné zavést k tomu, aby dané schéma mohlo plnit svůj účel. Pro pevnou hodnotu klíče nazýváme takto získaný mechanizmus *instancí* daného kryptografického schématu. Kryptografická schémata, ve kterých se využívají klíče, označujeme jako *klíčově závislá*, zkráceně *klíčovaná*.

Kryptoanalýza
cryptanalysis

Věda zabývající se primárně hledáním slabin *kryptografických schémat* a jejich luštěním.

Kryptografie
cryptography

Věda zabývající se primárně návrhem *kryptografických schémat*.

Kryptografické schéma
cryptographic scheme

Kryptografickým schématem nazýváme matematickou metodu, používanou k zajištění ochrany dat. Rozlišujeme čtyři základní cíle těchto ochran, které se nazývají: *důvěrnost*, *integrita*, *autentizace* a *nepopiratelnost*. Účelem důvěrnosti je zajistit, aby neautorizovaný subjekt nebyl schopen zjistit obsah chráněné zprávy. Integritní metody zajišťují to, že neautorizovaný subjekt není schopen chráněnou informaci nedetekovatelně změnit. Autentizační metody se dále dělí na *autentizaci původu zprávy* a *autentizaci subjektu*. Do první z uvedených podkategorií řadíme metody umožňující prokazatelným způsobem spojit konkrétní identitu subjektu s konkrétní chráněnou zprávou. Toto spojení je provedeno tak, že každá neautorizované změna v chráněné zprávě, či v identifikátoru připojené identity je detekovatelná. Do druhé podkategorie pak náleží schémata, která umožňují ověřit, že danému subjektu náleží jistá konkrétní identita. S takovými schématy se nejčastěji setkáme při přihlašování uživatelů do informačních systémů apod. Zajištění nepopiratelnosti se vztahuje ke konkrétním výrokům o chráněných informacích. O daném výroku řekneme, že je nepopiratelný, pokud pro nezávislou třetí stranu existuje způsob, jak se jednoznačně (se zanedbatelnou pravděpodobností omylu) přesvědčit o tom, že daný výrok platí, respektive neplatí. Příkladem takového výroku může být například: „Uživatel *A* podepsal datovou zprávu *m*.“ Třetí nezávislou stranou z uvedené definice bývá nejčastěji soud.

V praxi se většinou kryptografická schémata kombinují a spojují takovým způsobem, abychom z elementárních, úzce zaměřených funkcí, získali požadovanou komplexní metodu ochrany dat. Je vhodné si uvědomit, že schéma navržené k určitému konkrétnímu cíli (například k zajištění důvěrnosti) nemusí nutně plnit ostatní ochranné cíle (například zajištění integrity).

Kryptologie
cryptology

Interdisciplinární obor slučující *kryptografii* a *kryptoanalýzu*.

Podpisové schéma
signature scheme

Asymetrické kryptografické schéma zajišťující *autentizaci původu* chráněných dat. Takto chráněná data nazýváme *podepsanou zprávou* a subjekt, jehož identita je ke zprávě tímto schématem připojena, se nazývá *autorem podpisu*. Vlastní proces připojení autorovy identity nazýváme *podepsáním zprávy*. Proces prokázání tohoto spojení nazýváme *ověřením podpisu zprávy*. Dále požadujeme nepopiratelnost výroku o tom, že konkrétní subjekt konkrétní zprávu podepsal, respektive nepodepsal. Poznamenejme, že z uvedené definice plyne, že podpisové schéma implicitně zajišťuje také integritu podepsané zprávy.
V současnosti mezi nejpoužívanější podpisová schémata patří RSA, DSA a ECDSA, která jsou například v USA společně schválena standardem FIPS PUB 186-2, vydaným autoritou NIST.

Postranní kanál
side channel

Postranním kanálem nazýváme každý nežádoucí způsob výměny informací mezi kryptografickým modulem a jeho okolím. V současnosti rozeznáváme zejména kanály časové, napěťově-proudové, elektromagnetické, chybové a kleptografické.

Privátní klíč
private key

Utajovaný klíč v asymetrických kryptografických schématech. Ve většině schémat se požaduje jednoznačné přiřazení konkrétních privátních klíčů konkrétním subjektům.

RNG, PRNG

Termínem *Random Number Generator* (RNG) v kryptografii nazýváme zdroj nezávislých náhodných čísel, jejichž pravděpodobnostní rozdělení není dostupnými statistickými testy odlišitelné od *rovnoměrného rozdělení*. RNG založený na náhodných procesech fyzikální povahy (radioaktivní rozpad, kvantově mechanické děje, atp.) někdy speciálně označujeme termínem *true*-RNG (TRNG). RNG, jehož základní podstatou je splnění uvedených statistických testů zejména díky využití složitých matematických operací, označujeme termínem *pseudo*-RNG (PRNG). Pro některé zvláště citlivé aplikace se použití PRNG díky útokům plynoucím z jeho architektury obecně nepovažuje za dostatečnou záruku bezpečnosti.

Rovnoměrné rozdělení
uniform distribution

O náhodné veličině říkáme, že má rovnoměrné rozdělení, jestliže každá její hodnota má stejnou pravděpodobnost výskytu.

Symetrické kryptografické schéma
symmetric cryptographic scheme

Klíčově závislé schéma, ve kterém platí, že všechny subjekty, které společně používají konkrétní *instanci* tohoto schématu, rovněž společně sdílí konkrétní hodnotu klíče, která musí být pro správnou funkci schématu utajena.

Šifrovací schéma
encryption scheme

Symetrické či asymetrické kryptografické schéma sloužící primárně k zajištění důvěrnosti chráněných dat. Zkráceně tato schémata označujeme jako *šifry*.

ÚOOÚ

Úřad pro ochranu osobních údajů. Tento právní subjekt měl dříve na starost úpravu problematiky elektronického podpisu v ČR. Tento úkol nyní zastává Ministerstvo informatiky (zřízeno k 1.1. 2003)

Veřejný klíč
public key

Neutajovaný klíč v asymetrických kryptografických schématech. Ve většině schémat se požaduje jednoznačné přiřazení konkrétních veřejných klíčů konkrétním identitám subjektů. K tomuto účelu se často používají *certifikáty veřejných klíčů*.

Reference

S. A. Brands: *Rethinking Public Key Infrastructures and Digital Certificates*, The MIT Press, 2000
C. Clapham: *The Concise Oxford Dictionary of Mathematics*, Oxford University Press, 1996
A. Menezes, P. van Oorschot, and S. Vanstone: *Handbook of Applied Cryptography*, CRC Press, 1996