

一种基于椭圆曲线的短波数据通信身份认证机制

赵 亮¹, 雷 静²

(1 空军工程大学 工程学院, 陕西 西安 710038; 2 解放军 93897 部队, 陕西 西安 710077)

摘 要: 结合短波信道的特点, 比较了各种加密体制和算法, 进行了加密体制选择和加密算法选择, 最终确立一套切实可行的集加密与身份认证于一身的安全方案, 并给出了具体实现流程. 实现的加密认证方案对于解决短波数据通信中的安全问题有一定的参考价值.

关键词: 短波; 椭圆曲线; 身份认证

中图分类号: TN92

文献标识码: A

文章编号: 1000-7180(2010)05-0132-04

A HF Data Communication Identity Authentication Mechanism Base on Ellipse Curve System

ZHAO Liang¹, LEI Jing²

(1 Engineering College, Air Force University of Engineering, Xi'an 710038, China;

2 Military Unit 93897 of PLA, Xi'an 710077, China)

Abstract: The development of current encryption and authentication system is analyzed, cooperated with characteristics of HF channel, various kind of encryption system are compared and selected to construct an applicable mechanism of digital communication security, the flow chart of this system is provided by this paper too. The mechanism provided has some reference value for solving security problems in HF data communication.

Key words: HF; ellipse curve; identity authentication

1 引言

短波通信几乎是唯一能够提供抗毁的、廉价的远距离并且带宽相对较宽(与中长波相比)的利用无线电短波来进行通信的无线电通信手段. 短波数据通信具有设备简单、传输距离远、易于机动等优点, 被广泛用于军队、气象、林业等各个部门, 用以传送语音和数据.

由于短波通信的固有特点, 短波通信也存在很多的缺点: 短波信道的时变特性, 其信道容量有限, 同时速率相对较慢且信道不稳定, 这使得短波通信的可靠性受到很大的影响; 报文在短波信道传输的过程中, 具有相同频率的其它短波电台都可以对报文进行接收和截取等. 因此短波通信中安全保密和防伪问题成为人们关注的一个重要问题.

在信息安全的理论体系中, 认证和加密是两个重要的分支. 加密的作用在于保证通信过程中信息的私有性, 防止敌方获取信息. 而认证是为了确保信息通信的合法性和完整性. 在安全系统中这两个方面即是相互独立又存在密切关系, 可以根据安全需求实现一个或两个功能.

在短波通信中, 不管信息加密还是其它安全技术, 都必须基于身份认证的实现上, 身份认证技术在保证通信安全与网络安全领域占据极其重要的地位^[1-3].

2 身份认证技术

身份认证技术就是在信息网络、电子交易等环境下, 通过认证系统的验证、核实^[4-5], 来鉴别用户身份真实性和有效性的技术^[6].

在通信过程中,信息传至接收方后,接收方首先要确认信息发送方的合法身份,然后才能与之建立一条通信链路.通过建立身份认证系统,可实现网络用户的集中统一授权,防止未经授权的非法用户使用网络资源.

文中确立的身份认证方案基于对称密码体制与非对称密码体制,在进行短波通信过程中的工作量将大幅减小,加密效率有较大提高.

(1) 基于对称密钥算法的身份认证

对称密钥认证协议主要用在无仲裁认证的情况,通信双方相互信任,并且共享同一个秘密密钥,下面介绍一个典型的基于对称密钥的双向认证协议.

步骤1:用户随机选取一个随机数 R , 计算 $KC1 = EK_i(R)$, 接着利用用户自己的 ID , 计算 $KC = EK1(ID)$, 得到会话密钥 KC . 经过两级密钥分散隐藏了用户的秘密密钥.

步骤2:用户 A 利用分组加密算法,以 KC 为密钥计算 M 的单向数列值 $HKC(M)$, 以 3DES 算法为例,每个输入消息 M 的分组为 8 字节,如果不足 8 个字节就补零,超过的话采用 CBC 模式计算其单向散列值.

步骤3:用户 A 到用户 B 发送 $M \parallel ID \parallel R \parallel H_{kc}(M)$, 其中 $\parallel$ 表示消息的串联.

步骤4:用户 B 收到后,用用户 A 的秘密 K_i 重复步骤1~3的计算,如果算出来的 $HKC(M)$ 值和收到一样,就可以证明消息的完整性.由于用户 B 清楚只有用户 A 知道 K_i , 所以也可以证明消息是由用户 A 发送来的.

同理如果用户 A 需要验证用户 B 的身份,用户 B 也只需要对发送的消息进行步骤1~3的计算即可证明消息的合法性.

(2) 公钥算法的身份认证

基于公钥密码系统的数据传送流程是:当用户 A 要向用户 B 传送数据时,首先用户 A 用自己不公开的私钥来签名欲传送给用户 B 的数据,再用用户 B 所公开出来的公钥来进行加密,最后传送给用户 B . 当用户 B 收到此加密数据使用自己的私钥解开数据,因为只有用户 B 拥有其私钥,所以只有用户 B 能解密,接下来用户 B 取得用户 A 的公钥来验证解密后的消息的完整性和合法性.为了防止公钥篡改,可采用以数字证书为基础的公钥密码系统(Certificate-based public key cryptosystem),这个密码系统通过可信的第三方(Trusted Third Party, TTP)来

保证公钥的有效性.这就是著名的公钥基础设施(PKI).

短波通信中的身份认证方案基于以上两种模型的,只有很好的掌握这两种流程才能确立选用哪一种更合适.

3 认证方案设计

短波信道的特点是信道速率低,误码率高,短波通信身份认证机制要适应短波信道的特点.基于非对称密码体制的身份认证运算过程很复杂,也很耗时间,用在低速率的短波通信中效果可能不理想,而且使用对称密码体制进行信息认证职能保护通信双方不受第三方攻击,但不能防止通信双方的一方对另一方进行欺骗或伪造.所以文中采取基于公钥密码体制的身份认证方法,就是利用椭圆曲线加密算法来进行身份认证.认证要完成的功能有:(1)完整性;(2)新鲜性;(3)防抵赖功能;(4)秘密信息的管理与生成.

基于公钥的认证主要利用数字签名和哈希函数来实现.假设有通信双方 A 和 B , A 要发送信息给 B , A 先对信息 M 进行哈希运算 $Hash(M)$, 然后用私钥对哈希结果进行签名得到 $Sig_{SK_A}(Hash(M))$. A 将信息 $(M \parallel Sig_{SK_A}(Hash(M)))$ 发送给用户 B , B 通过 A 的公钥来验证 A 的私钥签名,从而确认信息的来源.然后通过对信息 M 作 $Hash(M)$ 并与解密后的哈希值作对比,以验证信息的完整性.用这种方法不但可以确定信息来源和验证信息的完整性,还可以提供防抵赖功能,因为 A 的私钥只有 A 才知道.但由于该方法是用 A 的私钥签名,而 A 的公钥又是公开的,因此该方法并不能对信息进行保密.公钥信息认证框图如图1所示.

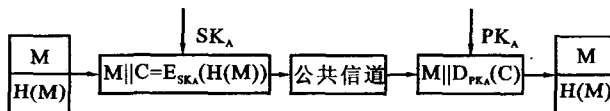


图1 公钥信息认证框图

如需同时提供加密和认证则可用如下方法: A 先用自己的私钥 SK_A 对 $H(M)$ 进行签名,再用接收方 B 的公钥 PK_B 进行加密, $C = E_{PK_B}[M \parallel E_{SK_A}(Hash(M))]$. 公钥加密认证框图如图2所示.

根据上述关于公钥加密认证流程,可以确定具体认证方案,即利用椭圆曲线算法对要传送的信息进行数字签名,基本的过程如下:现有通信双方 A 和 B , 这时 A 要发送信息给 B , 而且所发送信息需要

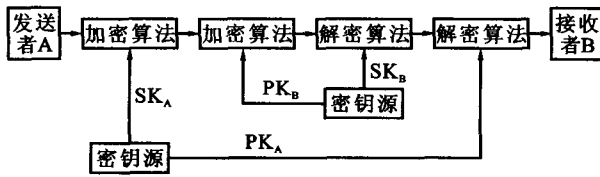


图2 公钥加密认证框图

经过加密, A 先对将要传送的信息 M 进行哈希运算, 然后用由椭圆曲线算法得到的私钥对哈希结果进行签名. A 将经过签名的信息发送给用户 B, B 收到 A 发送过来的信息后, 通过 A 的公钥来验证 A 的私钥签名, 从而确认信息的来源. 然后通过对信息 M 作 $\text{Hash}(M)$ 并与解密后的哈希值作对比, 以验证信息的完整性.

4 认证方案实现

4.1 各部分方案

每次通信中, 均使用一个 128 位 AES 密钥加密文件, 这个 128 位密钥是消息发送方随机产生的, 即使是同一文件, 两次加密结果也不相同, 以保证加密的可靠性. 接下来是用密钥扩展程序对密钥加以扩展. 128 位对应 $\text{Key Expansion}_{128}(\text{key})$, 生成 72bytes 的扩展密钥^[7-8].

AES 加密密钥用接收方的 160 位的椭圆曲线公钥进行加密后同信息一起传送, 仅接收方能使用自己的私钥进行解密, 其他人无法解密. 这一步就是确定椭圆曲线算法的具体参数. 首先要给出椭圆曲线域的参数来确定一条椭圆曲线. 在 IEEE P1363 标准中, 定义其参数为一个七元组: $T = (q, FR, a, b, G, n, h)$, 其中 q 代表有限域 $GF(q)$, q 为素数或 $2m$; FR 为域表示法, 如 $f(x)$ 为 F_{2m} 域元素的不可约多项式的表示法; 曲线的方程, 当 q 为素数时, 方程为 $y^2 = x^3 + ax + b$, 当 $q = 2m$ 时, 方程 $y^2 + xy = x^3 + ax^2 + b$, 其中 a, b 是方程中的系数; G 为基点; n 为大素数并且等于点 G 的阶, h 是小整数称为余因子且 $h = \#E(Fq)/n$. 主要的安全性参数 n , 因此 ECC 密钥的长度就定义为 n 的长度. 确定参数后, 选取椭圆曲线的方法是随机选取曲线法. 随机选取曲线的参数 $a, b \in Fq$ (如果 q 是素数则满足 $4a^3 + 27b^2 \neq 0$; 如果 $q = 2m$, 则 $b \neq 0$), 然后计算 $u = \#E(Fq)$ 和大素数因子 n , 直到所选曲线满足安全需求. 选取了基域 Fq 和椭圆曲线后, 得到了在有限域 Fq 上的曲线 E 确定的具体的形式, 即上述的椭圆曲线域参数的一个七元组. 每个用户选取一个整数 $d (1 \leq d \leq n)$ 作为其私钥, 而以点 $Q =$

dG (G 为基点) 作其公钥, 这样就形成一个椭圆曲线公钥密码系统. 在这个密码体制中, 具体的曲线, 基域 Fq , 基点 G 及其阶 n , 以及每个用户的公钥都是该系统的公开参数, 每个用户的私钥是保密的.

用哈希函数对信息进行哈希运算, 是为了收方收到信息后, 用哈希运算值与解密后的哈希值进行比较, 如果一样就证明信息传送是完整的. 哈希函数是一种单向密码体制, 它是一个从明文到密文的不可逆函数, 是无法解密的. 哈希函数 $H(M)$ 作用于任意长度的消息 M , 它返回一固定长度的散列值 $h = H(M)$ 作为初始消息独一无二的“数字指纹”, 从而能保证数据的完整性和唯一性. 大多数的单向散列函数产生 128 位的散列值. 单向函数有 SHA-1、MD5、MD2、RIPEMD-160 等. SHA-1 算法输入长度小于 264 位的消息时, 产生一个 160 位输出, 输入消息以 512 位的分组为单位进行处理. 对 SHA-1 还没有已知的密码攻击, 它比 128 位值数函数更有效抵抗穷举攻击. 在这选用 SHA-1 对数据进行摘要, 从而进行完整性验证.

在报文中附加发报当时的日期和时间, 以防止第三方重发, 避免被欺骗. 因为一旦信息被附加上发报当时的日期和时间之后, 第三方再想重放, 收方就会发现收包时间与上面所附发报时间不一样, 这样就会保证通信的安全性.

4.2 认证流程

整个认证流程如图 3 所示. 设进行短波通信的双方 A 和 B, A 要向 B 传送消息, 而且信息不想让其他人知道, 这就要求 A 要对信息进行签名并加密.

(1) 发方 A 先对明文 M 用 SHA-1 算法对原始报文产生 160 位的报文摘要, 该摘要保证了报文不能被篡改, 然后在明文中附上发送日期与时间. 再就是 A 利用本方通过椭圆曲线算法产生的私钥 SK_A 对 M 进行数字签名 (这个私钥 SK_A 只有 A 自己知道, 接收者就可以通过 A 的公钥来验证信息的来源, 防止 A 抵赖).

(2) 通过随机数生成器生成 128 位随机密钥 K , 并通过它用 AES 算法对明文 M 和经过数字签名的明文摘要一起进行加密得到密文 M_1 . 同时将随机数生成器生成的 128 位随机密钥 K 利用收方 B 的 160 位的椭圆曲线公钥 PK_B 进行加密.

(3) 将上述进行过加密的文件通过不安全的信道传送给 B, B 收到消息以后, 先是对用 PK_B 进行过加密的密钥通过收方 B 的 SK_B 进行解密, 得到 AES 解密密钥 K . 同时利用解密密钥 K 对密文 M_1

