(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 102 44 727 B4** 2008.01.10

(12) **Patentschrift**

(21) Aktenzeichen: **102 44 727.6**
(22) Anmeldetag: **25.09.2002**
(43) Offenlegungstag: **30.04.2003**
(45) Veröffentlichungstag
der Patenterteilung: **10.01.2008**

(51) Int Cl.[8]: ***H04L 9/28*** (2006.01)

(30) Unionspriorität:
09/975,815 11.10.2001 US

(73) Patentinhaber:
Hewlett-Packard Development Co., L.P., Houston, Tex., US

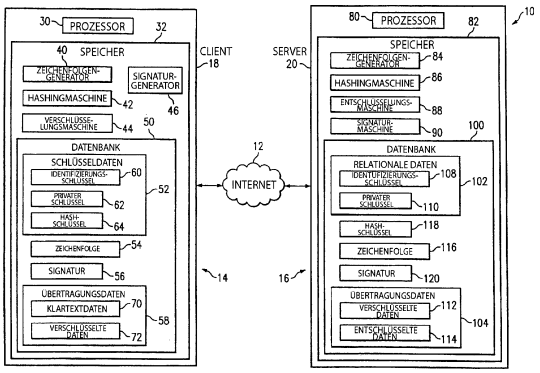
(74) Vertreter:
Schoppe, Zimmermann, Stöckeler & Zinkler, 82049 Pullach

(72) Erfinder:
Krawetz, Neal A., Fort Collins, Col., US

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
DE 198 22 795 A1
US 61 78 508 B1
CALLAS,J., et.al.: OpenPGP Message Format. RFC 2440, November 1998, S.1-65;

(54) Bezeichnung: **System und Verfahren zur sicheren Datenübertragung**

(57) Hauptanspruch: Verfahren zur sicheren Datenübertragung, mit folgenden Schritten:
Erzeugen einer Zeichenfolge (54) bei einem Sender (14);
Erzeugen eines Hash-Schlüssels (64) unter Verwendung der Zeichenfolge (54) und eines privaten Schlüssels (62);
Verschlüsseln der Daten (70) unter Verwendung des Hash-Schlüssels (64);
Erzeugen einer Signatur (56) unter Verwendung des Hash-Schlüssels (64) und der Daten (70); und
Übertragen eines Identifizierungsschlüssels (60), der dem Sender (14) zugeordnet ist, der Zeichenfolge (54), der verschlüsselten Daten (72) und der Signatur (56) von dem Sender (14) zu einem Empfänger (16).



Beschreibung

[0001] Die vorliegende Erfindung bezieht sich allgemein auf das Gebiet der Datenverarbeitung und insbesondere auf ein System und ein Verfahren zur sicheren Datenübertragung.

[0002] Das Internet ist ein beliebter Weg zur Datenübertragung geworden. Eine beträchtliche Menge an Daten jedoch, die über das Internet übertragen werden, kann empfindlicher oder vertraulicher Natur sein. So werden empfindliche oder vertrauliche Daten, die über das Internet übertragen werden, oft zum Schutz verschlüsselt und unter Verwendung eines Zertifikates, das allgemein durch eine Zertifizierungsautorität ausgegeben wird, authentifiziert. Verschlüsselte Datenübertragungen und Zertifikate jedoch leiden an mehreren Nachteilen. Sicherheitssockelschichten (SSL = Secure Socket Layer) z. B. verwenden Zertifikate auf Zeitbasis. Da die eingestellte Zeit zu jedem Ende der Datenübertragung z. B. zwischen einem Sender und einem Server unterschiedlich sein kann, können gültige Zertifikate unkorrekterweise abgelaufen sein oder abgelaufene Zertifikate unabsichtlich akzeptiert werden. Web-Browser können konfiguriert sein, um einem Benutzer ein ungültiges Zertifikat zu melden. Viele Benutzer jedoch können z. B. das Zertifikat einfach akzeptieren, ohne den Zweck des Zertifikates oder die Konsequenzen des Akzeptierens eines ungültigen Zertifikates zu verstehen. Zusätzlich erfordern automatisierte Sender allgemein eine in Hardware codierte Antwort. Folglich kann, wenn ein ungültiges Zertifikat akzeptiert wird, die Datenübertragung u. U. einem Abfangen durch Dritte unterworfen sein. Ferner muß allgemein, wenn das Zertifikat zurückgewiesen wird, eine Bestimmung hinsichtlich dessen gemacht werden, wo ein gültiges Zertifikat zu erhalten ist.

[0003] Die Patentveröffentlichung US 6,178,508 B1 betrifft eine Vorrichtung zum Steuern des Zugriffs auf gesicherte Daten durch Quoren von berechtigten Benutzern, von denen jeder ein Passwort hat, wobei die gesicherten Daten verschlüsselt und in einem Speicher gespeichert werden, wobei die Vorrichtung Folgendes umfasst: Mittel zum Erzeugen einer Tabelle im Speicher, die einen Eintrag für jeden aus der Vielzahl von berechtigten Benutzern aufweist, wobei der erste Eintrag einen verschlüsselten Hash-Wert des Passwortes von jedem Benutzer enthält; Mittel zum Verschlüsseln der gesicherten Daten, wobei sie im Speicher gespeichert werden; Mittel zum Empfangen einer Vielzahl von Passwörtern von einer Gruppe von Benutzern; Mittel zum Erzeugen von verschlüsselten Hash-Werten für jedes der empfangenen Passwörter; Mittel, die auf jedes verschlüsselte Hash-Passwort ansprechen, um den entsprechenden Benutzer als einen berechtigten Benutzer zu kennzeichnen, wenn das empfangene verschlüsselte Hash-Passwort mit irgendeinem der verschlüsselten Hash-Passwörter im Speicher übereinstimmt. Die Vorrichtung umfasst nun insbesondere ferner Mittel, die auf Passwörter ansprechen, die von einer Gruppe von berechtigten Benutzern empfangen wurden, deren verschlüsseltes Hash-Passwort mit irgendeinem der verschlüsselten Hash-Passwörter im Speicher übereinstimmt, um festzustellen, ob die Gruppe von berechtigten Benutzern ein gültiges Quorum bildet; und Mittel zum Entschlüsseln der gesicherten Daten, wenn die Gruppe von berechtigten Benutzern ein gültiges Quorum bildet.

[0004] Die Patentveröffentlichung DE 19822795 A1 betrifft ein Verfahren, mit dem ein Sitzungsschlüssel zwischen einer ersten Computereinheit und einer zweiten Computereinheit vereinbart werden kann, ohne daß ein unbefugter Dritter nützliche Informationen bezüglich der Schlüssel oder der Identität der ersten Computereinheit erhalten kann. Dies wird erreicht durch die Einbettung des Prinzips des El-Gamal Schlüsselaustauschs in das Verfahren mit einer zusätzlichen Bildung einer digitalen Unterschrift über einen Hash-Wert, dessen Eingangsgröße mindestens Größen, aus denen auf den Sitzungsschlüssel eindeutig rückgeschlossen werden kann, aufweist.

[0005] Es ist die Aufgabe der vorliegenden Erfindung, ein verbessertes Verfahren für eine sichere Datenübertragung oder ein System zur sicheren Datenübertragung mit verbesserten Charakteristika zu schaffen.

[0006] Diese Aufgabe wird durch ein Verfahren gemäß Anspruch 1 oder 10 oder ein System gemäß Anspruch 17 oder 24 gelöst.

[0007] Gemäß einem Ausführungsbeispiel der vorliegenden Erfindung weist ein Verfahren zur sicheren Datenübertragung ein Erzeugen einer Zeichenfolge bei einem Sender, ein Erzeugen eines Hash-Schlüssels unter Verwendung der Zeichenfolge und eines privaten Schlüssels und ein Verschlüsseln der Daten unter Verwendung des Hash-Schlüssels auf. Das Verfahren weist außerdem ein Übertragen eines Identifizierungsschlüssels, der dem Sender zugeordnet ist, der Zeichenfolge und der verschlüsselten Daten von dem Sender an einen Empfänger auf.

[0008] Gemäß einem weiteren Ausführungsbeispiel der vorliegenden Erfindung weist ein System zur sicheren Datenübertragung einen Prozessor, einen Speicher, der mit dem Prozessor gekoppelt ist, und einen Zeichenfolgengenerator auf, der in dem Speicher gespeichert und durch den Prozessor ausführbar ist. Der Zeichenfolgengenerator ist angepaßt, um eine Zeichenfolge zu erzeugen. Das System weist außerdem eine Hashing-Maschine auf, die in dem Speicher gespeichert und durch den Prozessor ausführbar ist. Die Hashing-Maschine ist angepaßt, um einen Hash-Schlüssel unter Verwendung der Zei-

chenfolge und eines privaten Schlüssels zu erzeugen. Das System weist ferner eine Verschlüsselungsmaschine auf, die in dem Speicher gespeichert und durch den Prozessor ausführbar ist. Die Verschlüsselungsmaschine ist angepaßt, um die Daten unter Verwendung des Hash-Schlüssels zu verschlüsseln. Der Prozessor ist angepaßt, um die verschlüsselten Daten, einen Identifizierungsschlüssel, der auf den privaten Schlüssel bezogen ist, und die Zeichenfolge an einen Empfänger zu senden.

[0009] Gemäß einem weiteren Ausführungsbeispiel der vorliegenden Erfindung weist ein Verfahren zur sicheren Datenübertragung ein Empfangen einer Zeichenfolge und eines Identifizierungsschlüssels von dem Sender auf. Das Verfahren weist außerdem ein Empfangen verschlüsselter Daten von dem Sender auf. Das Verfahren weist ferner ein Bestimmen eines privaten Schlüssels, der dem Sender zugeordnet ist, unter Verwendung des Identifizierungsschlüssels und ein Entschlüsseln der verschlüsselten Daten unter Verwendung des privaten Schlüssels und der Zeichenfolge auf.

[0010] Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend Bezug nehmend auf die beigefügten Zeichnungen näher erläutert, in denen gleiche Bezugszeichen für gleiche und entsprechende Teile der verschiedenen Zeichnungen verwendet werden. Es zeigen:

[0011] Fig. 1 ein Diagramm, das ein System zur sicheren Datenübertragung gemäß einem Ausführungsbeispiel der vorliegenden Erfindung darstellt;

[0012] Fig. 2 ein Flußdiagramm, das ein Verfahren zur sicheren Datenübertragung gemäß einem Ausführungsbeispiel der vorliegenden Erfindung darstellt; und

[0013] Fig. 3 ein Flußdiagramm, das ein Verfahren zur sicheren Datenübertragung gemäß einem Ausführungsbeispiel der vorliegenden Erfindung darstellt.

[0014] Fig. 1 ist ein Diagramm, das ein System **10** zur sicheren Datenübertragung gemäß einem Ausführungsbeispiel der vorliegenden Erfindung darstellt. Bei dem dargestellten Ausführungsbeispiel werden Informationen oder Daten über das Internet **12** zwischen einem Sender **14** und einem Empfänger **16** kommuniziert. In dem dargestellten Ausführungsbeispiel weisen z. B. der Sender **14** und der Empfänger **16** einen Clienten **18** auf, der über das Internet **12** mit einem Server **20** kommuniziert. Es wird jedoch darauf verwiesen, daß andere Kommunikationskomponenten und andere Kommunikationsmedien, wie z. B., jedoch nicht ausschließlich, lokale Netze oder Großraumnetze, ebenso verwendet werden können. Zusätzlich kann, wie unten weiter beschrieben wird, die vorliegende Erfindung für eine sichere Datenübertragung von dem Clienten **18** zu dem Server **20** oder von dem Server **20** zu dem Clienten **18** verwendet werden.

[0015] Bei dem dargestellten Ausführungsbeispiel weist der Client **18** einen Prozessor **30** auf, der mit einem Speicher **32** gekoppelt ist. Die vorliegende Erfindung umfaßt außerdem eine Computersoftware, die in dem Speicher **32** gespeichert und durch den Prozessor **30** ausgeführt werden kann. Bei diesem Ausführungsbeispiel weist der Client **18** einen Zeichenfolgengenerator **40**, eine Hashing-Maschine **42**, eine Verschlüsselungsmaschine **44** und einen Signaturgenerator **46** auf, die Computersoftwareprogramme sind. In Fig. 1 sind der Zeichenfolgengenerator **40**, die Hashing-Maschine **42**, die Verschlüsselungsmaschine **44** und der Signaturgenerator **46** dargestellt, um in dem Speicher **32** gespeichert zu sein, wo dieselben durch den Prozessor **30** ausgeführt werden können. Kurz gesagt werden der Zeichenfolgengenerator **40**, die Hashing-Maschine **42** und die Verschlüsselungsmaschine **44** verwendet, um die Daten zu verschlüsseln, die durch den Clienten **18** zu dem Server **20** übertragen werden sollen. Der Signaturgenerator **46** erzeugt eine Signatur zum Übertragen von dem Clienten **18** an den Server **20** zum Authentifizieren der Datenübertragung und der Identität des Clienten **18**.

[0016] Der Client **18**, der in Fig. 1 dargestellt ist, weist außerdem eine Datenbank **50** auf. Bei dem dargestellten Ausführungsbeispiel weist die Datenbank **50** Schlüsseldaten **52**, Zeichenfolgendaten **53**, Signaturdaten **56** und Übertragungsdaten **58** auf. Die Schlüsseldaten **52** weisen Informationen auf, die Schlüsseln zugeordnet sind, die verwendet werden, um den Clienten **18** zu identifizieren und die Daten zu verschlüsseln und zu entschlüsseln, die von dem Clienten an den Server **20** übertragen werden. Bei dem dargestellten Ausführungsbeispiel z. B. weisen die Schlüsseldaten **52** einen Identifizierungsschlüssel **60** auf, der verwendet wird, um den Clienten **18** zu identifizieren. Der Identifizierungsschlüssel **60** kann z. B. eine Seriennummer oder einen anderen Typ von Identifizierer aufweisen, der den bestimmten Clienten **18** anzeigt, der die Daten überträgt. Die Schlüsseldaten **52** weisen außerdem einen privaten Schlüssel **62** und einen Hash-Schlüssel **64** auf. Kurz gesagt wird der Hash-Schlüssel **64** unter Verwendung des privaten Schlüssels **62** erzeugt. Der Hash-Schlüssel **64** wird dann verwendet, um die übertragenen Daten zu verschlüsseln und zu entschlüsseln.

[0017] Bei dem dargestellten Ausführungsbeispiel weisen die Übertragungsdaten **58** unverschlüsselte Daten **70** und verschlüsselte Daten **72** auf. Die Daten **70** weisen Informationen auf, die durch einen Benutzer des Clienten **18** bereitgestellt werden und in einem unverschlüsselten oder entschlüsselten Format

an den Server **20** übertragen werden sollen. Die verschlüsselten Daten **72** weisen ein verschlüsseltes Format der Daten **70** auf, die über das Internet **12** an den Server **20** übertragen werden.

[0018] In Betrieb erzeugt der Zeichenfolgengenerator **40** die Zeichenfolge **54** zufällig und speichert dieselbe in der Datenbank **50**. Die Hashing-Maschine **42** unterzieht die Zeichenfolge **54** einem Hashing mit dem privaten Schlüssel **62**, um den Hash-Schlüssel **64** zu erzeugen, der ebenfalls in der Datenbank **50** gespeichert ist. Die Verschlüsselungsmaschine **44** verschlüsselt dann die Daten **70** unter Verwendung des Hash-Schlüssels **64** als einem Verschlüsselungspaßwort. Wie oben kurz erläutert wurde, können die verschlüsselten Daten **72** auch in der Datenbank **50** gespeichert sein. Der Prozessor **30** überträgt dann die Zeichenfolge **54**, die verschlüsselten Daten **72** und den Identifizierungsschlüssel **60** über das Internet **12** an den Server **20**. Die Entschlüsselung der verschlüsselten Daten **72** durch den Server **20** wird weiter unten detaillierter beschrieben. Zusätzlich wird darauf verwiesen, daß, obwohl sie als eine „Verschlüsselungs"-Maschine **44** identifiziert ist, die Verschlüsselungsmaschine **44** verwendet werden kann, um Daten zu verschlüsseln oder zu entschlüsseln. Die vorliegende Erfindung kann jedoch auch unter Verwendung separater Verschlüsselungs- und Entschlüsselungskomponenten konfiguriert sein.

[0019] Der Signaturgenerator **46** erzeugt die Signatur **56** und speichert dieselbe in der Datenbank **50** durch ein Hashing des Hash-Schlüssels **64** mit den Daten **70**. Der Prozessor **30** überträgt außerdem die Signatur **56** über das Internet **12** an den Server **20**. Eine Authentifizierung oder Verifizierung der übertragenen Daten und der Identität des Clienten **18** durch den Server **20** unter Verwendung der Signatur **56** wird weiter unten detaillierter beschrieben.

[0020] Bei dem dargestellten Ausführungsbeispiel weist der Server **20** außerdem einen Prozessor **80** auf, der mit einem Speicher **82** gekoppelt ist. Die vorliegende Erfindung umfaßt außerdem Computersoftware, die in dem Speicher **82** gespeichert und durch den Prozessor **80** ausgeführt werden kann. Bei diesem Ausführungsbeispiel weist der Server **20** einen Zeichenfolgengenerator **84**, eine Hashing-Maschine **86**, eine Entschlüsselungsmaschine **88** und eine Signaturmaschine **90** auf, die Computersoftwareprogramme sind. In Fig. 1 sind der Zeichenfolgengenerator **84**, die Hashing-Maschine **86**, die Entschlüsselungsmaschine **88** und die Signaturmaschine **90** dargestellt, um in dem Speicher **82** gespeichert zu sein, wo dieselben durch den Prozessor **80** ausgeführt werden können. Kurz gesagt werden die Hashing-Maschine **86**, die Entschlüsselungsmaschine **88** und die Signaturmaschine **90** verwendet, um die Daten, die von dem Clienten **18** empfangen werden, zu entschlüsseln und zu verifizieren oder authentifizieren. Der Zeichenfolgengenerator **84** wird zur Erzeugung einer zufälligen Zeichenfolge in Verbindung mit einem Übertragen von Daten von dem Server **20** an den Clienten **18** auf eine ähnliche Weise, die oben beschrieben ist, verwendet. Zusätzlich wird darauf verwiesen, daß, obwohl sie als „Entschlüsselungs"-Maschine **88** identifiziert ist, die Entschlüsselungsmaschine **88** verwendet werden kann, um Daten zu verschlüsseln oder zu entschlüsseln.

[0021] Der Server **20** weist außerdem eine Datenbank **100** auf, die durch den Prozessor **80** zugänglich ist. Beidem dargestellten Ausführungsbeispiel weist die Datenbank **100** relationale Daten **102** und Übertragungsdaten **104** auf. Die relationalen Daten **102** weisen Informationen auf, die einer Beziehung von Verschlüsselungs- und Entschlüsselungsschlüsseln für jeden der Clienten **18** zu den übertragenen Identifizierungsschlüssel **60** zuordnet sind. Bei dem dargestellten Ausführungsbeispiel z. B. weisen die relationalen Daten **102** Identifizierungsschlüssel **108** und private Schlüssel **110** auf, die in einer Nachschlagtabelle oder einem anderen Format angeordnet sind, derart, daß für jeden Identifizierungsschlüssel **108** ein zusammenpassender oder entsprechender privater Schlüssel **110** identifiziert werden kann. Folglich sind die Identifizierungsschlüssel **60** und **108** und die privaten Schlüssel **62** und **110** so korreliert, daß eine Datenverschlüsselung und -Entschlüsselung an jedem Ende des Datenübertragungspfades durchgeführt werden kann.

[0022] Die Übertragungsdaten **104** weisen Informationen auf, die den Daten zugeordnet sind, die von dem Clienten **18** empfangen werden. Bei dem dargestellten Ausführungsbeispiel z. B. weisen die Übertragungsdaten **104** verschlüsselte Daten **112** und entschlüsselte Daten **114** auf. Die verschlüsselten Daten **112** weisen die Informationen auf, die in einer verschlüsselten Form von dem Clienten **18** über das Internet **12** empfangen werden. Folglich weisen die entschlüsselten Daten **114** die Informationen auf, die nach einer Entschlüsselung unter Verwendung der Entschlüsselungsmaschine **88** über das Internet **12** von dem Clienten **18** empfangen werden. Die entschlüsselten Daten **114** können jedoch auch Informationen in einem nicht verschlüsselten Format aufweisen, die von dem Server **20** an den Clienten **18** übertragen werden sollen.

[0023] In Betrieb empfängt der Server **20** die Zeichenfolge **54** von dem Clienten **18** und speichert die Zeichenfolge **54** als eine Zeichenfolge **116** in der Datenbank **100**. Unter Verwendung des Identifizierungsschlüssels **60**, der von dem Clienten **18** empfangen wird, greift der Prozessor **80** auf die relationalen Daten **102** der Datenbank **100** zu, um den privaten Schlüssel **110**, der dem Identifizierungsschlüssel **60** entspricht, zu bestimmen. Wie oben beschrieben wurde, können die relationalen Daten **102** z. B. eine

Nachschlagtabelle aufweisen, die jeden Identifizierungsschlüssel **108** auf einen privaten Schlüssel **110** bezieht. Unter Verwendung des Identifizierungsschlüssels **60** kann ein entsprechender Identifizierungsschlüssel **108** identifiziert werden, wodurch auch der entsprechende private Schlüssel **110** identifiziert wird. Die Hashing-Maschine **86** erzeugt einen Hash-Schlüssel **118** und speichert denselben in der Datenbank **100** durch ein Hashing des privaten Schlüssels **110** mit der Zeichenfolge **116**. Die Entschlüsselungsmaschine **88** entschlüsselt dann die verschlüsselten Daten **112** unter Verwendung des Hash-Schlüssels **118**. Die entschlüsselten Daten **114** werden dann in der Datenbank **100** gespeichert.

[0024] Um die übertragenen Daten und die Identität des Clienten **18** zu authentifizieren, wird die Signaturmaschine **90** verwendet, um die Signatur **56**, die von dem Clienten **18** empfangen wird, zu verifizieren oder authentifizieren. In Betrieb führt die Signaturmaschine **90** ein Hashing bezüglich des Hash-Schlüssels **118** mit den entschlüsselten Daten **114** durch, um eine Signatur **120** zu erzeugen, die in der Datenbank **100** gespeichert ist. Die Signatur **120** kann dann mit der Signatur **56** verglichen werden, um die übertragenen Daten und die Identität des Clienten **18** zu verifizieren und zu authentifizieren. Wenn die Signatur **120** nicht mit der Signatur **56** übereinstimmt, kann der Prozessor **80** konfiguriert sein, um eine Warnung oder einen Alarm gegenüber einem Benutzer des Systems **10** zu erzeugen und/oder die Übertragungsdaten **104** zu verwerfen.

[0025] Die vorliegende Erfindung kann auch verwendet werden, um Daten von dem Server **20** über das Internet **12** zu dem Clienten **18** zu übertragen. Der Zeichenfolgengenerator **84** kann z. B. verwendet werden, um zufällig eine Zeichenfolge **116** zu erzeugen und in der Datenbank **100** zu speichern. Die Hashing-Maschine **86** kann ein Hashing bezüglich des privaten Schlüssels **110**, der dem Clienten **18** entspricht, mit der Zeichenfolge **116** durchführen, um den Hash-Schlüssel **118** zu erzeugen. Unter Verwendung des Hash-Schlüssels **118** kann die Maschine **88** verwendet werden, um Daten zu verschlüsseln, die zu dem Clienten **18** übertragen werden sollen. Die verschlüsselten Daten und die Zeichenfolge **116** werden dann von dem Server **20** über das Internet **12** an den Clienten **18** übertragen. Der Client **18** kann dann die Daten unter Verwendung der Zeichenfolge **116** und des privaten Schlüssels **62** entschlüsseln, ähnlich wie oben in Verbindung mit dem Server **20** beschrieben wurde. Die Hashing-Maschine **42** kann z. B. verwendet werden, um die Zeichenfolge **116**, die durch den Generator **84** erzeugt wird, mit dem privaten Schlüssel **62** einem Hashing zu unterziehen, um den Hash-Schlüssel **64** zum Entschlüsseln der empfangen verschlüsselten Daten **112** zu erzeugen. Die Signaturmaschine **90** kann auch verwendet werden, um eine Signatur **120** zu erzeugen, die den übertragenen Daten entspricht, indem der Hash-Schlüssel **118** mit den Daten einem Hashing unterzogen wird, ähnlich wie oben in Verbindung mit dem Clienten **18** beschrieben wurde. Die Signatur **120** kann dann über das Internet **12** zu dem Clienten **18** übertragen werden. Der Client **18** kann dann die Signatur **120** mit einer Signatur vergleichen, die durch den Signaturgenerator **46** unter Verwendung des Hash-Schlüssels **64** und der entschlüsselten Daten erzeugt wurde. Die Prozessoren **30** und **80** können auch konfiguriert sein, um eine Folgenummer oder einen Identifizierer in die Daten **70** und **114** einzuschließen, derart, daß eine doppelte Datenübertragung oder eine Datenübertragung außerhalb der Reihenfolge, die entweder durch den Clienten **18** oder den Server **20** empfangen werden, verworfen oder zurückgewiesen wird.

[0026] Fig. 2 ist ein Flußdiagramm, das ein Verfahren zur sicheren Datenübertragung gemäß einem Ausführungsbeispiel der vorliegenden Erfindung darstellt. Das Verfahren beginnt bei Schritt **200**, an dem der Identifizierungsschlüssel **60** in der Datenbank **50** gespeichert wird. Bei Schritt **204** wird auch der private Schlüssel **62**, der dem Clienten **18** entspricht, in der Datenbank **50** gespeichert. Der Client **18** empfängt Daten, die über das Internet **12** zu dem Server **20** übertragen werden sollen, bei Schritt **206**. Bei Schritt **208** erzeugt der Zeichenfolgengenerator **40** eine zufällige Zeichenfolge **54** und speichert die Zeichenfolge **54** in der Datenbank **50**. Bei Schritt **210** erzeugt die Hashing-Maschine **42** den Hash-Schlüssel **64** durch ein Hashing des privaten Schlüssels **62** mit der Zeichenfolge **54**. Bei Schritt **212** verschlüsselt die Verschlüsselungsmaschine **44** die Daten **70**, die zu dem Server **20** übertragen werden sollen, unter Verwendung des Hash-Schlüssels **64** als einem Verschlüsselungspaßwort.

[0027] Bei Schritt **214** erzeugt der Signaturgenerator **46** die Signatur **56** durch ein Hashing des Hash-Schlüssels **64** mit den Daten **70**. Die Zeichenfolge **54**, die verschlüsselten Daten **72**, der Identifizierungsschlüssel **60**, der dem Clienten **18** entspricht, und die Signatur **56** werden dann bei Schritt **216** über das Internet **12** zu dem Server **20** übertragen.

[0028] Fig. 3 ist ein Flußdiagramm, das ein Verfahren zur sicheren Datenübertragung gemäß einem weiteren Ausführungsbeispiel der vorliegenden Erfindung darstellt. Das Verfahren beginnt bei Schritt **300**, bei dem Identifizierungsschlüssel **108**, die jedem Clienten **18** entsprechen, in der Datenbank **100** gespeichert werden. Bei Schritt **302** werden außerdem private Schlüssel **110**, die auf jeden der Identifizierungsschlüssel **108** bezogen sind, in der Datenbank **100** gespeichert. Bei Schritt **304** empfängt der Server **20** die Zeichenfolge **54**, die verschlüsselten Daten **72**, den Identifizierungsschlüssel **60**, der dem übertragenden Clienten **18** entspricht, und die Signatur **56**

von dem Clienten **18**.

[0029] Bei Schritt **306** greift der Prozessor **80** auf die relationalen Daten **102** der Datenbank **100** zu. Bei Schritt **308** wird der empfangene Identifizierungsschlüssel **60** des Clienten **18** verwendet, um den privaten Schlüssel **110** zu bestimmen, der dem Clienten **18** entspricht. Bei Schritt **310** erzeugt die Hashing-Maschine **86** den Hash-Schlüssel **118** durch ein Hashing des privaten Schlüssels **110** mit der Zeichenfolge **54**, die von dem Clienten **18** empfangen wird. Bei Schritt **312** entschlüsselt die Entschlüsselungsmaschine **88** die verschlüsselten Daten **72**, die von dem Clienten **18** empfangen werden, unter Verwendung des Hash-Schlüssels **118** und speichert die entschlüsselten Daten **114** in der Datenbank **100**. Bei Schritt **314** erzeugt die Signaturmaschine **90** die Signatur **120** durch ein Hashing des Hash-Schlüssels **318** mit den entschlüsselten Daten **114**.

[0030] Bei Schritt **316** wird die erzeugte Signatur **120** mit der empfangenen Signatur **56** verglichen, um die empfangenen Daten zu verifizieren und zu authentifizieren. Bei einem Entscheidungsschritt **318** wird eine Bestimmung durchgeführt, ob die Signatur **120** mit der Signatur **56** übereinstimmt. Wenn die Signatur **120** mit der Signatur **56** übereinstimmt, endet das Verfahren. Wenn die Signatur **120** nicht mit der Signatur **56** übereinstimmt, fährt das Verfahren von Schritt **318** zu Schritt **320** fort, an dem die entschlüsselten Daten **114** verworfen werden können. Zusätzlich kann eine Warnung, die anzeigt, daß die Signatur **120** nicht mit der Signatur **56** übereinstimmt, bei Schritt **322** erzeugt werden.

[0031] So liefert die vorliegende Erfindung eine sichere Datenübertragung, ohne Zertifikate oder andere, durch Dritte bereitgestellte Informationen zu erfordern. Folglich reduziert oder eliminiert die vorliegende Erfindung die Wahrscheinlichkeit eines Abfangens durch Dritte und einer Untergrabung der übertragenen Daten wesentlich. Zusätzlich wird, da die vorliegende Erfindung keine Verwendung von Zertifikaten auf Zeitbasis umfaßt, das Verlassen auf Systemtakten und das blinde Akzeptieren potentiell ungültiger Zertifikate im wesentlichen beseitigt. Ferner verändert sich der Verschlüsselungsschlüssel im Gegensatz zu sicheren Shell- oder anderen Tunnelprotokollen mit jedem übertragenen Datenpaket, wodurch weiter die Wahrscheinlichkeit eines Abfangens durch Dritte oder einer Untergrabung reduziert wird.

[0032] Es wird darauf verwiesen, daß bei den beschriebenen Verfahren bestimmte Schritte weggelassen oder in einer anderen Reihenfolge als der, die in den Fig. 2 und Fig. 3 dargestellt ist, erzielt werden können. Bezug nehmend auf Fig. 2 z. B. kann Schritt **208** des Erzeugens der Zeichenfolge **54** zu jedem Zeitpunkt vor Schritt **210** des Erzeugens des Hash-Schlüssels **54** erzielt werden. Ferner wird darauf verwiesen, daß die in den Fig. 2 und Fig. 3 dargestellten Verfahren verändert werden können, um jedes der anderen Merkmale oder Aspekte der Erfindung zu umfassen, die an anderer Stelle in der Spezifizierung beschrieben sind.

Patentansprüche

1. Verfahren zur sicheren Datenübertragung, mit folgenden Schritten:
Erzeugen einer Zeichenfolge (**54**) bei einem Sender (**14**);
Erzeugen eines Hash-Schlüssels (**64**) unter Verwendung der Zeichenfolge (**54**) und eines privaten Schlüssels (**62**);
Verschlüsseln der Daten (**70**) unter Verwendung des Hash-Schlüssels (**64**);
Erzeugen einer Signatur (**56**) unter Verwendung des Hash-Schlüssels (**64**) und der Daten (**70**); und
Übertragen eines Identifizierungsschlüssels (**60**), der dem Sender (**14**) zugeordnet ist, der Zeichenfolge (**54**), der verschlüsselten Daten (**72**) und der Signatur (**56**) von dem Sender (**14**) zu einem Empfänger (**16**).

2. Verfahren gemäß Anspruch 1, bei dem das Erzeugen des Hash-Schlüssels (**64**) ein Hashing der Zeichenfolge (**54**) mit dem privaten Schlüssel (**62**) aufweist.

3. Verfahren gemäß einem der Ansprüche 1 bis 2, bei dem das Erzeugen einer Zeichenfolge (**54**) ein zufälliges Erzeugen der Zeichenfolge (**54**) aufweist.

4. Verfahren gemäß einem der Ansprüche 1 bis 3, das ferner folgende Schritte aufweist:
Bestimmen des privaten Schlüssels (**62**) an dem Empfänger (**16**) unter Verwendung des Identifizierungsschlüssels (**60**); und
Entschlüsseln der verschlüsselten Daten (**72**) an dem Empfänger (**16**) unter Verwendung des privaten Schlüssels (**62**) und der Zeichenfolge (**54**).

5. Verfahren gemäß Anspruch 4, bei dem das Bestimmen des privaten Schlüssels (**62**) ein Zugreifen auf eine relationale Datenbank (**102**) aufweist, die den Identifizierungsschlüssel (**60**) dem privaten Schlüssel (**62**) zuordnet.

6. Verfahren gemäß einem der Ansprüche 1 bis 3, das ferner folgende Schritte aufweist:
Bestimmen des privaten Schlüssels (**62**) an dem Empfänger (**16**) unter Verwendung des Identifizierungsschlüssels (**60**);
Bestimmen des Hash-Schlüssels (**64**) an dem Empfänger (**16**) unter Verwendung des privaten Schlüssels (**62**) und der Zeichenfolge (**54**); und
Entschlüsseln der verschlüsselten Daten (**72**) unter Verwendung des Hash-Schlüssels (**64**).

7. Verfahren gemäß Anspruch 6, bei dem das Be-

stimmen des Hash-Schlüssels (**64**) ein Hashing des privaten Schlüssels (**62**) mit der Zeichenfolge (**54**) aufweist.

8. Verfahren gemäß Anspruch 1, das ferner folgende Schritte aufweist:
Erzeugen einer ersten Signatur (**56**) durch den Sender (**14**) unter Verwendung des Hash-Schlüssels (**64**) und der Daten (**70**); und
Übertragen der ersten Signatur (**56**) an den Empfänger (**16**), wobei der Empfänger (**16**) angepaßt ist, um den Hash-Schlüssel (**64**) zum Entschlüsseln der Daten (**70**) zu bestimmen und die erste Signatur (**56**) mit einer zweiten Signatur (**120**), die durch den Empfänger (**16**) unter Verwendung des Hash-Schlüssels (**64**) und der entschlüsselten Daten (**114**) erzeugt wird, zu vergleichen.

9. Verfahren gemäß Anspruch 1, das ferner folgende Schritte aufweist:
Bestimmen des privaten Schlüssels (**62**) an dem Empfänger (**16**) unter Verwendung des Identifizierungsschlüssels (**60**);
Bestimmen des Hash-Schlüssels (**64**) an dem Empfänger (**16**) unter Verwendung des privaten Schlüssels (**62**) und der Zeichenfolgen (**54**);
Entschlüsseln der verschlüsselten Daten (**72**) an dem Empfänger (**16**) unter Verwendung des Hash-Schlüssels (**64**); und
Verifizieren der Signatur (**56**) an dem Empfänger (**16**) unter Verwendung des Hash-Schlüssels (**64**) und der entschlüsselten Daten (**114**).

10. Verfahren zur sicheren Datenübertragung, mit folgenden Schritten:
Empfangen einer Zeichenfolge (**54**) von einem Sender (**14**);
Empfangen eines Identifizierungsschlüssels (**60**) von dem Sender (**14**);
Empfangen verschlüsselter Daten (**72**) von dem Sender (**14**);
Empfangen einer Signatur von dem Sender (**14**); und
Bestimmen eines privaten Schlüssels, der dem Sender (**14**) zugeordnet ist, unter Verwendung des Identifizierungsschlüssels (**60**);
Entschlüsseln der verschlüsselten Daten unter Verwendung des privaten Schlüssels und der Zeichenfolge; und
Verifizieren der Signatur unter Verwendung der entschlüsselten Daten, des privaten Schlüssels und der Zeichenfolge.

11. Verfahren gemäß Anspruch 10, das ferner ein Bestimmen eines Hash-Schlüssels unter Verwendung der Zeichenfolgen und des privaten Schlüssels aufweist, und bei dem das Entschlüsseln der verschlüsselten Daten ein Entschlüsseln der verschlüsselten Daten unter Verwendung des Hash-Schlüssels aufweist.

12. Verfahren gemäß Anspruch 10 oder 11, bei dem das Bestimmen des privaten Schlüssels ein Zugreifen auf eine relationale Datenbank (**102**) aufweist, die den Identifizierungsschlüssel dem privaten Schlüssel zuordnet.

13. Verfahren gemäß einem der Ansprüche 10 bis 12, bei dem das Empfangen der Zeichenfolge ein Empfangen einer zufällig erzeugten Zeichenfolge aufweist.

14. Verfahren gemäß einem der Ansprüche 10 bis 13, das ferner ein Hashing der Zeichenfolge mit dem privaten Schlüssel aufweist, um einen Hash-Schlüssel zu erzeugen, und bei dem das Entschlüsseln der verschlüsselten Daten ein Entschlüsseln der verschlüsselten Daten unter Verwendung des Hash-Schlüssels aufweist.

15. Verfahren gemäß einem der Ansprüche 10 bis 14, das ferner folgende Schritte aufweist:
Bestimmen eines Hash-Schlüssels unter Verwendung des privaten Schlüssels und der Zeichenfolge; und
Verifizieren der Signatur unter Verwendung der entschlüsselten Daten und des Hash-Schlüssels.

16. Verfahren gemäß einem der Ansprüche 10 bis 14, das ferner folgende Schritte aufweist:
Bestimmen eines Hash-Schlüssels unter Verwendung des privaten Schlüssels und der Zeichenfolge;
Erzeugen einer zweiten Signatur unter Verwendung des Hash-Schlüssels und der entschlüsselten Daten; und
Vergleichen der ersten Signatur mit der zweiten Signatur.

17. System zur sicheren Datenübertragung, mit folgenden Merkmalen:
einem Prozessor (**30**);
einem Speicher (**32**), der mit dem Prozessor gekoppelt ist;
einem Zeichenfolgengenerator (**40**), der in dem Speicher gespeichert und durch den Prozessor (**30**) ausführbar ist, wobei der Zeichenfolgengenerator angepaßt ist, um eine Zeichenfolge (**54**) zu erzeugen;
einer Hashing-Maschine (**42**), die in dem Speicher gespeichert und durch den Prozessor ausführbar ist, wobei die Hashing-Maschine angepaßt ist, um einen Hash-Schlüssel unter Verwendung der Zeichenfolge und eines privaten Schlüssels (**62**) zu erzeugen; und
einer Verschlüsselungsmaschine (**44**), die in dem Speicher gespeichert und durch den Prozessor ausführbar ist, wobei die Verschlüsselungsmaschine angepaßt ist, um die Daten unter Verwendung des Hash-Schlüssels (**64**) zu verschlüsseln, und
einer Signaturmaschine (**46**), die in dem Speicher gespeichert und durch den Prozessor ausführbar ist, wobei die Signaturmaschine angepaßt ist, um eine Signatur unter Verwendung des Hash-Schlüssels

(**64**) und der Daten zu erzeugen, wobei der Prozessor ferner angepaßt ist, um die Signatur an den Empfänger (**16**) zu übertragen;
wobei der Prozessor angepaßt ist, um die verschlüsselten Daten (**72**), einen Identifizierungsschlüssel (**60**), der auf den privaten Schlüssel (**62**) bezogen ist, und die Zeichenfolge (**54**) an einen Empfänger (**16**) zu übertragen.

18. System gemäß Anspruch 17, bei dem der Empfänger (**16**) angepaßt ist, um die verschlüsselten Daten (**72**) zu entschlüsseln und die Signatur unter Verwendung der entschlüsselten Daten zu verifizieren.

19. System gemäß einem der Ansprüche 17 bis 18, bei dem die Hashing-Maschine (**42**) angepaßt ist, um die Zeichenfolge (**54**) einem Hash-Verfahren mit dem privaten Schlüssel zu unterziehen, um den Hash-Schlüssel (**64**) zu erzeugen.

20. System gemäß einem der Ansprüche 17 bis 19, bei dem der Zeichenfolgengenerator (**40**) angepaßt ist, um zufällig eine Zeichenfolge zu erzeugen.

21. System gemäß einem der Ansprüche 17 bis 20, bei dem der Empfänger (**16**) angepaßt ist, um die verschlüsselten Daten unter Verwendung des Identifizierungsschlüssels und der Zeichenfolge zu entschlüsseln.

22. System gemäß einem der Ansprüche 17 bis 21, bei dem der Empfänger (**16**) angepaßt ist, um den Hash-Schlüssel unter Verwendung des Identifizierungsschlüssels und der Zeichenfolge zu bestimmen und die verschlüsselten Daten unter Verwendung des Hash-Schlüssels zu entschlüsseln.

23. System gemäß einem der Ansprüche 17 bis 22, bei dem der Empfänger (**16**) angepaßt ist, um auf eine relationale Datenbank (**102**) zuzugreifen, die den Identifizierungsschlüssel dem privaten Schlüssel zuordnet, und um die verschlüsselten Daten unter Verwendung des privaten Schlüssels und der Zeichenfolge zu entschlüsseln.

24. System zur sicheren Datenübertragung, mit folgenden Merkmalen:
einem Prozessor, der angepaßt ist, um verschlüsselte Daten, einen Identifizierungsschlüssel und eine Zeichenfolge von einem Sender (**14**) zu empfangen;
einem Speicher, der mit dem Prozessor gekoppelt ist;
einer relationalen Datenbank (**102**), die in dem Speicher gespeichert und durch den Prozessor zugänglich ist, wobei die relationale Datenbank den Identifizierungsschlüssel auf einen privaten Schlüssel bezieht;
einer Entschlüsselungsmaschine (**88**), die in dem Speicher gespeichert und durch den Prozessor ausführbar ist, wobei die Entschlüsselungsmaschine angepaßt ist, um die verschlüsselten Daten unter Verwendung der Zeichenfolge und des privaten Schlüssels zu entschlüsseln; und
einer Signaturmaschine (**90**), die in dem Speicher gespeichert und durch den Prozessor ausführbar ist, wobei die Signaturmaschine angepaßt ist, um eine Signatur, die von dem Sender (**14**) empfangen wird, unter Verwendung des privaten Schlüssels und der Zeichenfolge zu verifizieren.

25. System gemäß Anspruch 24, das ferner eine Hashing-Maschine aufweist, die in dem Speicher gespeichert und durch den Prozessor ausführbar ist, wobei die Hashing-Maschine angepaßt ist, um einen Hash-Schlüssel unter Verwendung des privaten Schlüssels und der Zeichenfolge zu erzeugen, wobei die Entschlüsselungsmaschine angepaßt ist, um die verschlüsselten Daten unter Verwendung des Hash-Schlüssels zu entschlüsseln.

26. System gemäß Anspruch 24, das ferner folgende Merkmale aufweist:
eine Hashing-Maschine, die in dem Speicher gespeichert und durch den Prozessor ausführbar ist, wobei die Hashing-Maschine angepaßt ist, um einen Hash-Schlüssel unter Verwendung des privaten Schlüssels und der Zeichenfolge zu erzeugen; und
wobei die Signaturmaschine angepaßt ist, um eine Signatur, die von dem Sender empfangen wird, unter Verwendung des Hash-Schlüssels und der entschlüsselten Daten zu verifizieren.

27. System gemäß Anspruch 24, das ferner eine Hashing-Maschine aufweist, die in dem Speicher gespeichert und durch den Prozessor ausführbar ist, wobei die Hashing-Maschine angepaßt ist, um die Zeichenfolge einem Hash-Verfahren mit dem privaten Schlüssel zu unterziehen, um einen Hash-Schlüssel zu erzeugen, wobei die Entschlüsselungsmaschine angepaßt ist, um die verschlüsselten Daten unter Verwendung des Hash-Schlüssels zu verschlüsseln.

28. System gemäß einem der Ansprüche 24 bis 27, das ferner einen Zeichenfolgengenerator aufweist, der in dem Speicher gespeichert und durch den Prozessor ausführbar ist, wobei der Zeichenfolgengenerator angepaßt ist, um eine Zeichenfolge zu erzeugen, und bei dem die Entschlüsselungsmaschine (**88**) ferner angepaßt ist, um Daten zur Übertragung zu dem Sender (**14**) unter Verwendung der Zeichenfolge und des privaten Schlüssels zu verschlüsseln.

29. System gemäß Anspruch 28, das ferner folgende Merkmale aufweist:
einen Zeichenfolgengenerator, der in dem Speicher gespeichert und durch den Prozessor ausführbar ist, wobei der Zeichenfolgengenerator angepaßt ist, um eine Zeichenfolge zu erzeugen; und

eine Hashing-Maschine, die in dem Speicher gespeichert und durch den Prozessor ausführbar ist, wobei die Hashing-Maschine angepaßt ist, um die Zeichenfolge einem Hash-Verfahren mit dem privaten Schlüssel zu unterziehen, um einen Hash-Schlüssel zu erzeugen, und bei dem die Entschlüsselungsmaschine (**88**) ferner angepaßt ist, um Daten zur Übertragung zu dem Sender (**14**) unter Verwendung des Hash-Schlüssels zu verschlüsseln.

30. System gemäß Anspruch 28 oder 29, wobei die Signaturmaschine angepaßt ist, um eine erste Signatur unter Verwendung der entschlüsselten Daten zu erzeugen und die erste Signatur mit einer zweiten Signatur zu vergleichen, die von dem Sender (**14**) empfangen wird.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

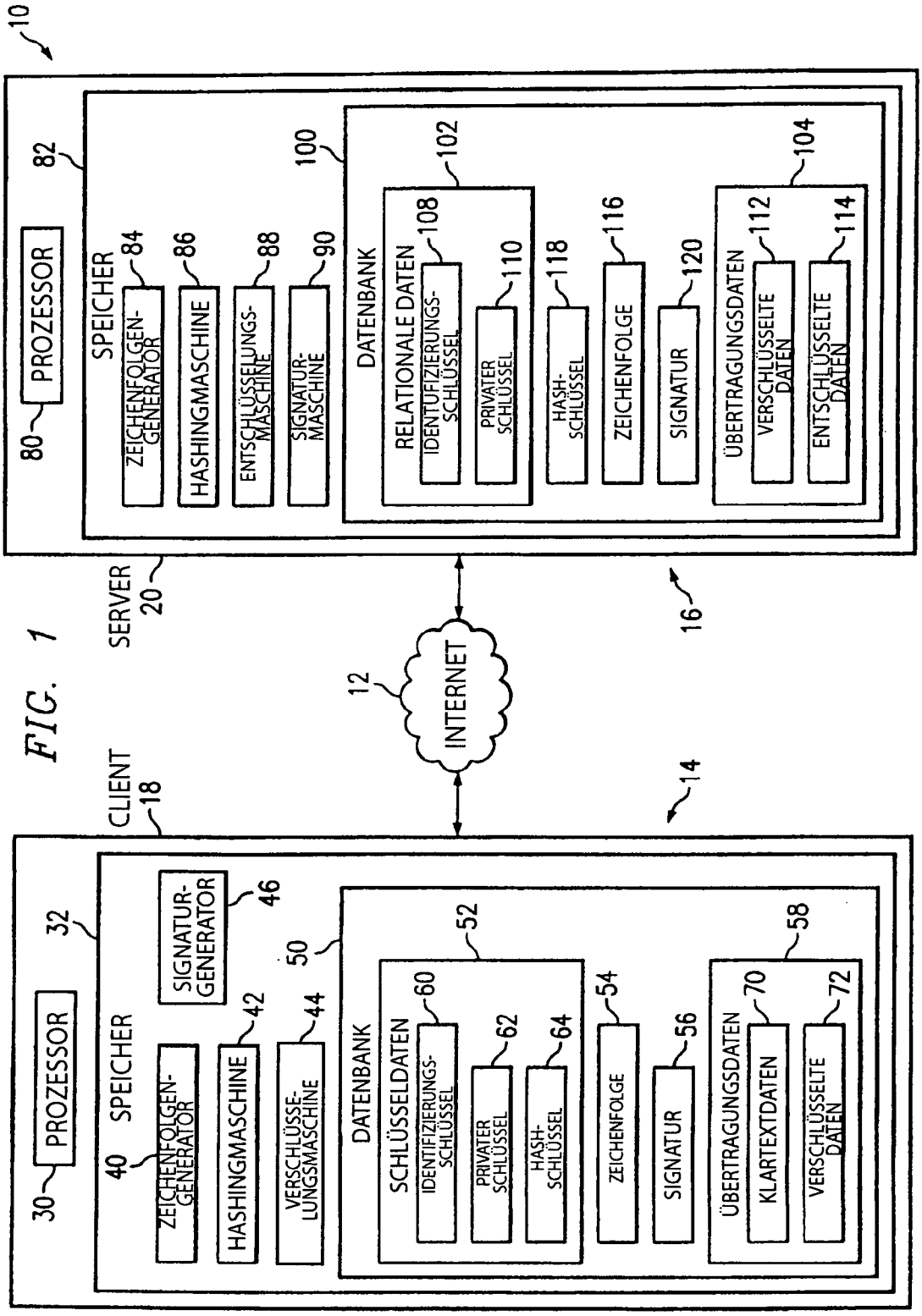


FIG. 1

FIG. 2

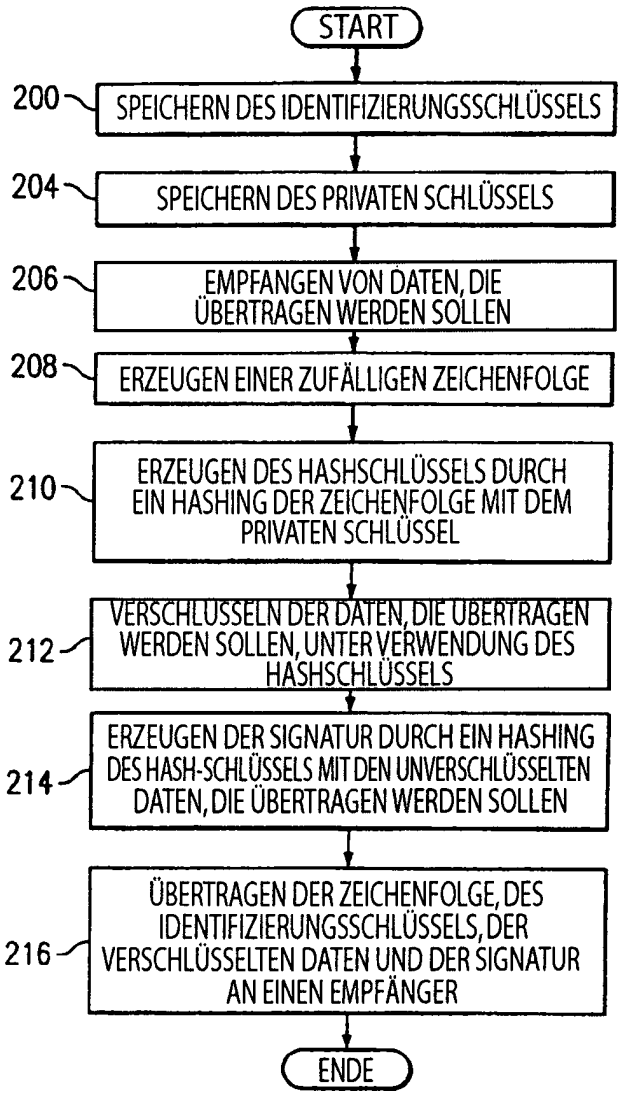
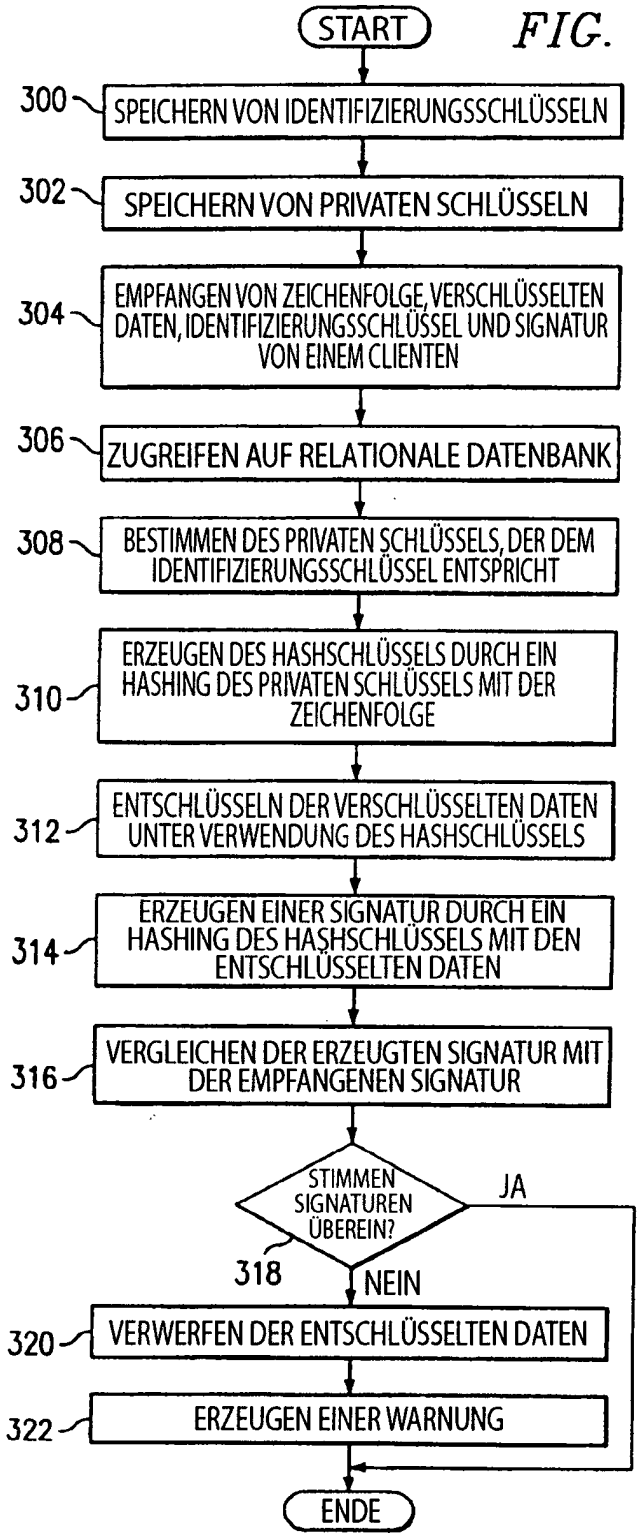

START
200
SPEICHERN DES IDENTIFIZIERUNGSSCHLÜSSELS
204
SPEICHERN DES PRIVATEN SCHLÜSSELS
206
EMPFANGEN VON DATEN, DIE ÜBERTRAGEN WERDEN SOLLEN
208
ERZEUGEN EINER ZUFÄLLIGEN ZEICHENFOLGE
210
ERZEUGEN DES HASHSCHLÜSSELS DURCH EIN HASHING DER ZEICHENFOLGE MIT DEM PRIVATEN SCHLÜSSEL
212
VERSCHLÜSSELN DER DATEN, DIE ÜBERTRAGEN WERDEN SOLLEN, UNTER VERWENDUNG DES HASHSCHLÜSSELS
214
ERZEUGEN DER SIGNATUR DURCH EIN HASHING DES HASH-SCHLÜSSELS MIT DEN UNVERSCHLÜSSELTEN DATEN, DIE ÜBERTRAGEN WERDEN SOLLEN
216
ÜBERTRAGEN DER ZEICHENFOLGE, DES IDENTIFIZIERUNGSSCHLÜSSELS, DER VERSCHLÜSSELTEN DATEN UND DER SIGNATUR AN EINEN EMPFÄNGER
ENDE

FIG. 3


START
300
SPEICHERN VON IDENTIFIZIERUNGSSCHLÜSSELN
302
SPEICHERN VON PRIVATEN SCHLÜSSELN
304
EMPFANGEN VON ZEICHENFOLGE, VERSCHLÜSSELTEN DATEN, IDENTIFIZIERUNGSSCHLÜSSEL UND SIGNATUR VON EINEM CLIENTEN
306
ZUGREIFEN AUF RELATIONALE DATENBANK
308
BESTIMMEN DES PRIVATEN SCHLÜSSELS, DER DEM IDENTIFIZIERUNGSSCHLÜSSEL ENTSPRICHT
310
ERZEUGEN DES HASHSCHLÜSSELS DURCH EIN HASHING DES PRIVATEN SCHLÜSSELS MIT DER ZEICHENFOLGE
312
ENTSCHLÜSSELN DER VERSCHLÜSSELTEN DATEN UNTER VERWENDUNG DES HASHSCHLÜSSELS
314
ERZEUGEN EINER SIGNATUR DURCH EIN HASHING DES HASHSCHLÜSSELS MIT DEN ENTSCHLÜSSELTEN DATEN
316
VERGLEICHEN DER ERZEUGTEN SIGNATUR MIT DER EMPFANGENEN SIGNATUR
STIMMEN SIGNATUREN ÜBEREIN?
318
JA
NEIN
320
VERWERFEN DER ENTSCHLÜSSELTEN DATEN
322
ERZEUGEN EINER WARNUNG
ENDE