AUSGABE 2/00

T.D.T.®
Transfer Data Test GmbH

T.D.T.-SPEZIAL
Telekommunikation in der Schweiz

- ***Telekursgruppe***
  Innovationen fuer den Finanzplatz und Wirtschaftsstandort Schweiz
- ***Swisscom***
  Vom Monopolisten zum Global Player
- ***ProEda AG***
  Das Konzept Tankomat 97 (TM97) mit TA-ALPHA erfolgreich
- ***COMTESYS Sarl***
  T.D.T.-Haendler Johann M. Hager betreut schweizerische Unternehmen

MICRO- und ALPHA-Router
Applikations-zeichnungen zeigen Einsatzmoeglichkeiten

T.D.T.-Event 2000
Michael Pickhardt und Sabine Laermann heirateten

Produktionsleitung wird personell verstaerkt
Juergen Siegl stellvertretender Produktionsleiter

Schulungen
Neue Termine auf Seite 4

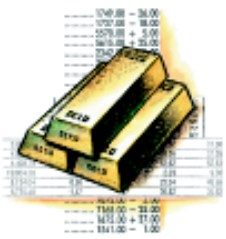
24-Stunden-Service
Support jetzt rund um die Uhr

Editorial

Last-Minute-News

Aufbruchstimmung in der Schweiz

In der Schweiz berühren sich Tradition und Zukunft. Obwohl klein an Fläche ist sie so attraktiv, dass sich die ganze Welt dort trifft - geschäftlich und zum Vergnügen. Das gilt auch für E-Commerce und die Telekommunikation. Die Szene ist noch überschaubar und hat mittlerweile hohes internationales Niveau erreicht. Vor allem im bedeutendsten Wirtschaftszentrum der Schweiz, in Zürich, bestimmen Newcomer und arrivierte Firmen das Geschehen. Die große Bedeutung der Stadt an der Limmat ist bekannt - so ist zum Beispiel hier der größte Goldumschlagplatz der Welt. Viele schweizerische Banken, wie auch die Schweizer Nationalbank, haben hier ihren Hauptsitz. Die traditionsbewusste Schweizer Börse in Zürich mit Börsenchefin Antoniette Hunizer konnte im Frühjahr 2000 einen gewaltigen Boom verzeichnen. Die durchschnittliche Börsenkapitalisierung des Schweizer Neuen Marktes liegt etwa auf demselben Niveau wie am Neuen Markt in Frankfurt und sogar deutlich über den Werten in Paris, Brüssel und Amsterdam. Viele schweizerische Firmen setzen dabei auf die Nutzung alter und neuer Kommunikationswege und *TDT* liefert in entscheidenden Bereichen die Bauteile. Exemplarisch für die eidgenössischen Unternehmen porträtiert *TDT* zwei.



TELEKURS

Die elektronische Drehscheibe des Finanzplatzes Schweiz

Die an der Züricher Hardturmstraße domizilierte Telekurs ist eine Unternehmensgruppe der schweizerischen Banken. In der Schweiz und auf ausländischen Finanzplätzen erbringt sie für Banken und Bankkunden marktorientierte Dienstleistungen auf den Gebieten Zahlungsmittel, Zahlungssysteme und Finanzinformationen. Die Telekurs-Gruppe beschäftigt über 1.700 Mitarbeiterinnen und Mitarbeiter, davon rund 270 im Ausland. Im Geschäftsjahr 1999 erarbeitete die Gruppe einen Betriebsertrag von CHF 717,9 Millionen und einen Cash Flow von CHF 130,4 Millionen.

Bargeldlose Zahlungsmittel und elektronische Zahlungssysteme

Die EUROPAY (Switzerland) SA ist das führende Unternehmen im schweizerischen Acquiring-Geschäft (Kartenakzeptanz beim Handel/Vertragspartner) mit dem Ziel, den sicheren und effizienten bargeldlosen Zahlungsverkehr zu fördern. Mit der Verarbeitung der EUROCARD/MasterCard als führende Kreditkarte, den Debitkarten ec und Maestro sowie der Wertkarte CASH bietet EUROPAY seinen Vertragspartnern einen erstklassigen, umfassenden und exklusiven „All in One"- Service aus einem Kompetenzzentrum an.

Auch in den Bereichen des elektronischen Zahlungsverkehrs (Zahlungssysteme) und E-Commerce verfügt EUROPAY mit den Produkten PayNet, DTA (Datenträgeraustausch) und LSV (Lastschriftverfahren) über innovative, zukunftsorientierte Dienstleistungen.

Processing von Bank- und Kartenzahlungen

Die Payserv AG erbringt umfassende Processing- und Logistikdienstleistungen für Banken und Kartenherausgeber sowie für andere Dienstleistungsunternehmen und betreibt sichere Informatikplattformen und Online-Applikationen in den Bereichen Finanzinformationen und Zahlungsverkehr.

Als führendes Verarbeitungscenter für Kredit-, Debit- und Wertkarten in der Schweiz bietet sie Banken und Kartenunternehmen maßgeschneiderte Processing-Lösungen für das Karteninhaber- und das Vertragspartnergeschäft an. Unter anderem betreibt und betreut sie die nationalen Systeme Bancomat, EFT/POS und CASH. Im E-Commerce-Markt nimmt Payserv als Anbieterin von Spezialitäten für Zahlungslösungen (SET Payment Gateway, SET Certificate Authority) eine Leaderrolle ein.

Umfassende Dienstleistungen erbringt Payserv auch in der Verarbeitung von Direct-Marketing-Programmen und in der Belegverarbeitung.

Die Payserv AG ist ferner für die technische und betriebliche Infrastruktur der gesamten Telekurs-Gruppe zuständig. Unter anderem betreibt sie eines der leistungsfähigsten Rechenzentren der Schweiz. Diese Dienstleistungen bietet sie auch Dritten an.

Clearingsysteme

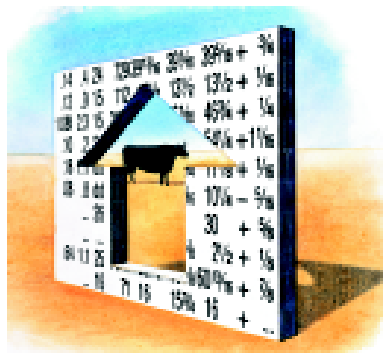
Die Telekurs SIC AG betreut das Swiss Interbank Clearing (SIC) sowie euroSIC, das Clearingsystem für Zahlungen in Euro in der Schweiz und über ihre Grenzen hinaus. Das Clearingsystem SIC ist seit 1987 das Herz des Franken-Zahlungsverkehrs der Banken in der Schweiz. SIC bildete auch die Basis bei der Realisierung von euroSIC.

Dank euroSIC können schweizerische Banken und Finanzinstitute seit dem 1. Januar 1999 in der Schweiz und grenzüberschreitend Zahlungen in Euro ausführen. Weil die Schweiz weder Mitglied der EU noch der EWU ist, besitzt die Schweizer Nationalbank keinen direkten Anschluss an TARGET, dem Clearingsystem der europäischen Zentralbanken. Um euroSIC trotzdem mit genügend Liquidität versorgen zu können betreibt die Telekurs Holding AG zusammen mit der UBS, der Credit Suisse Group

und Postfinance die SECB Swiss Euro Clearing Bank GmbH in Frankfurt/Main.

Finanzinformationen

Die Telekurs Finanzinformationen AG beliefert – als Anbieterin von internationalen Finanzinformationen – Anlageberater, Vermögensverwalter, Finanzanalysten, Portfoliomanager sowie Wertschriftenfachleute rund um den Erdball mit Real-time-Kursen, Wertpapierverwaltungsdaten und aktuellen Wirtschaftsnachrichten.



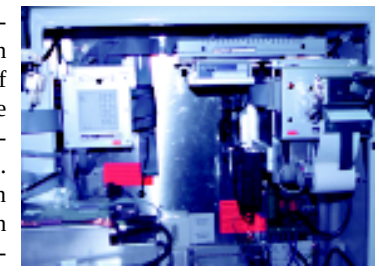
In Zusammenarbeit mit zehn Tochtergesellschaften in Europa, Asien und den USA unterhält sie eine der umfassendsten und modernsten Wertpapierdatenbank der Welt. Sie umfasst Real-time-Kurse und Wertpapierverwaltungsdaten von über 1,5 Millionen Titeln. Die Displayprodukte Finvest, FinXS, Finbase und Finphone WAP erlauben einen einfachen Zugriff auf das gesamte Datenangebot der Telekurs Finanzinformationen AG.

Seit mehr als fünf Jahren setzt EUROPAY auf *TDT*-Dienste. Der modulare Aufbau der DCCs der zweiten Generation ermöglicht das Routen der Daten von den POS-Geräten über die DCCs zu den Großrechnern. Für die sprichwörtliche schweizerische Präzision der *TDT*-Geräte spricht, dass vom Tag der Inbetriebnahme bis heute die Geräte ohne Ausfallzeiten und ohne Wartungsaufwand ihre Dienste verrichten. Mit einer doppelt so hohen Geschwindigkeit wie die Vorgängermodelle werden die Daten, ohne dass ein Byte verlorengeht, weitergeroutet. Die hohe Kanaldichte des DCC sorgt für ein sicheres Routing zu den Rechner-Applikationen. Nach fünf äußerst erfolgreichen Jahren können die Verantwortlichen sehr gut beurteilen, welches Know-how in der niederbayerischen Firma steckt. Sie schätzen vor allem die schnelle Reaktionszeit bei technischen Fragen. Die kompetente technische Unterstützung war unter anderem Anlass, auch Single PADs und TA-ALPHAS zu bestellen. Auch bei der Installation der Geräte bewährte sich der telefonische Support und die Konfiguration via Remote. Da im Bereich Clearing und speziell bei Europay gleichzeitig analoge und digitale Datenübertragungen stattfinden, bietet sich für das Unternehmen der DCC-Einwahlpool an. Ein Gerät ersetzt bis zu 30 Modems oder Terminaladapter. In Stoßzeiten können die Einwahlpools pro S_{2M}-Schnittstelle (Primäranschluss) bis zu dreißig B-Kanäle gleichzeitig belegen.

Auch bei neuen strategischen Ausrichtungen kann *TDT* in der Praxis erprobte Lösungen anbieten. So gewährleisten zum Beispiel *TDT*-Gateway-Lösungen bei der Datenübertragung über TCP/IP eine sichere und zuverlässige Anbindung der für das Kommunikationsprotokoll X.25 optimierten Großrechner an die Vermittlungsgeräte.

Die ProEda AG

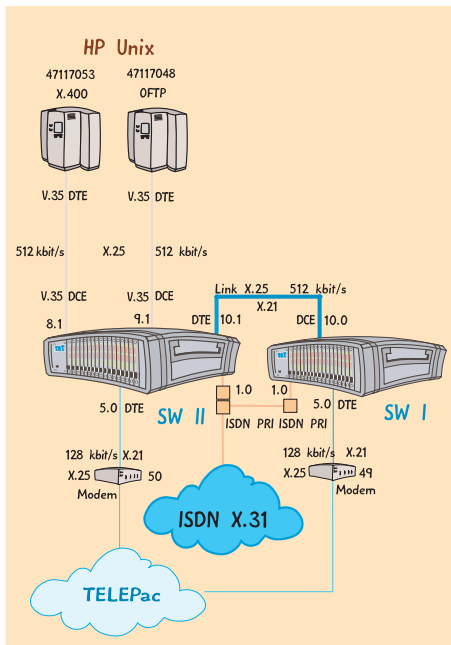
Einer der führenden Hersteller von Tankautomaten in der Schweiz ist kürzlich zur Gruppe der Frame Holding AG gestoßen. Das in der Nähe von Bern gelegene Unternehmen besticht seit 1964 durch innovative Konzepte in der Entwicklung und Herstellung von Automaten und Managementsystemen für Tankstellen. Mit dem Konzept Tankomat (TM 97) hat bei den Tankstellen die digitale Datenübertragung vom Automaten zum Clearingcenter Einzug gehalten.



Auf der Suche nach effizienten Terminaladaptern sind die Schweizer auf das niederbayerische Telekommunikationsunternehmen gestoßen. Die *TDT*-Geraete erfüllen die im Pflichtenheft von Telekurs vorgeschriebenen Anforderungen zur Kommunikationsanbindung der Tankstellen in der Schweiz mit höchster Kompetenz und bieten zusätzliche wertvolle Features an. Die in den Tankautomaten integrierten Terminaladapter (TA-ALPHA) sind seither fester Bestandteil der Datenübertragung zwischen Tankstelle und Payserve, der Clearingstelle für Kreditkarten von Telekurs.

swisscom

Wie die Deutsche Telekom hat auch die Swisscom den Weg vom Monopolisten zum modernen, im Wettbewerb stehenden Unternehmen gehen müssen. Die Ergebnisse sind nicht nur für die Eidgenossen erstaunlich positiv. Die Ausrichtungen sind klar erkennbar: die Swisscom hat sich in kurzer Zeit zu einem international tätigen Telekommunikationsunternehmen entwickelt.



Mit einem Nettoumsatz von rund 11,2 Milliarden Franken und ca. 22.000 Mitarbeitenden, davon 750 Auszubildende, ist der Swisscom-Konzern das führende Telekommunikationsunternehmen in der Schweiz. Der innovative, kundenorientierte und wettbewerbsstarke Konzern bietet umfassende Dienstleistungen in der mobilen und netzgebundenen Sprach- und Datenkommunikation an und ist im E-Business tätig. In diesen Feldern setzt die Swisscom seit Jahren *TDT*-Geräte ein.

Swisscom betreut in der Schweiz 3,6 Mio. analoge Festnetzanschlüsse, dazu über 1,3 Mio. ISDN-Kanäle. Die Schweiz weist im internationalen Vergleich eine der höchsten ISDN-Anschlussdichten auf. Swisscom Mobile steigerte allein 1999 ihre Kundenzahl um 36% auf über 2,3 Millionen Kunden. Bald jeder dritte Bewohner der Schweiz kommuniziert auf dem NATEL-Netz von Swisscom, das 98% des bewohnten Gebietes abdeckt.

Das Unternehmen bietet, von Mietleitungen bis hin zu integrierten Lösungen für Geschäftskunden, eine vollständige Palette modernster Datendienste an. Mit Blue Window, dem führenden Internet-Anbieter in der Schweiz, verfügt Swisscom über das größte Online-Portal für Privatkunden. Blue Window zählt über 440 000 Access- und 130 000 Blue-Mail-Kunden.

Mit einer klar formulierten Strategie will Swisscom auch in Zukunft ihre Marktführerschaft in der Schweiz behaupten und ein bedeutendes Wachstum im Ausland erzielen. Dabei konzentriert sich das Unternehmen auf die Wachstumsgeschäfte wie Mobilkommunikation, Internet und E-Business sowie auf die Vermarktung ihrer Netzleistungen (Wholesale) an Wiederverkäufer. Die 1999 erfolgte Akquisition von debitel, dem drittgrößten Mobilfunkanbieter in Deutschland und größten netzunabhängigen Dienstleister Europas, führte zu einer Verdoppelung des Swisscom-Kundenstamms auf über 10 Mio. Kunden und einer deutlichen Steigerung des Gesamtumsatzes.

Customerlösungen für eShops mit Mehrnutzen tragen zu dem guten Betriebsergebnis bei

Fallbeispiele:

Der Kunde (Shopper) wählt sich auf seinem PC über das Internet in einen von ihm angewählten Shop ein. Bei CommerceMaker Starter wird die meistverkaufte Shoppinglösung Intershop mit dem Betrieb (Hosting) in einer sicheren Swisscom-Umgebung erstmals kombiniert. Intershop ist eine Kataloglösung, mit der der Shopanbieter seine Produkte beliebig strukturiert und in Verbindung mit seiner Produktdatenbank im Internet präsentieren kann.

CommerceMaker Payment bietet eine komplette Umgebung für die Verarbeitung von elektronischen Transaktionen und beinhaltet Module wie z. B.: Order Management, Customer Service, Security sowie Customer Authentification.

Die CommerceMaker Payment-Lösung bietet Zahlungsmöglichkeiten für alle wichtigen Kreditkarten (Visa, MasterCard, Amex, Diners). Sehr beliebt ist auch eine automatische Verrechnung über die Swisscom Telefonrechnung, selbstverständlich mit separat ausgewiesenen Belastungen. Zahlungen für Klein- und Kleinstbeträge können entweder über die Swisscom Telefonrechnung oder über ein elektronisches Wallet beglichen werden. Bei einem elektronischen Wallet baut der Shopper über seine Kreditkarte ein Guthaben auf (Wallet), von dem seine Einkäufe abgebucht werden. Auch ist eine Rechnungsstellung möglich. Transaktionen können auch über das Postkonto abgewickelt werden.

Der Shopanbieter entscheidet natürlich selbst, welche Zahlungsmittel er seinen Kunden zur Verfügung stellen will. CommerceMaker Payment trennt die Websites mit dem Waren- oder Dienstleistungsangebot klar von der Bestell- und Zahlungstransaktion. CommerceMaker Payment kann auch auf einfache Weise an eine bereits bestehende Internet-Shopping-Lösung angebunden werden.

Paketorientierte Datenkommunikation

Das Prinzip der Paketvermittlung im Datenverkehr besteht darin, die Daten in Pakete aufzuteilen und diese über den bestmöglichen Weg zur Empfangsadresse zu senden. Diese Datenkommunikationsart wird in der Schweiz vor allem in den Bereichen EFTPos (Electronic File Transfer Point of Sales) zur Kreditkartenautorisierung, für Auskunfts- und Reservationsdienste, sowie zur Übertragung von Alarm- und Überwachungsdaten eingesetzt.

Im ISDN-Netz der Swisscom wird diese Übertragungsart, die eine X.25-Kommunikation sowohl über den B- als auch über den D-Kanal eines Basisanschlusses (S_0) ermöglicht, unter dem Namen ISDNPac angeboten.

Der Service beruht auf dem durch das ITU-T beschriebene „Packet Mode Bearer Service (PMBS)“, definiert in der Empfehlung X.31 CASE B. Damit wird eine X.25-Kommunikation über ISDN ermöglicht.

Im B-Kanal beträgt die maximale Übertragungsrate 64 kbit/s, im D-Kanal 9,6 kbit/s. Wird der D-Kanal verwendet, sind die beiden B-Kanäle des ISDN-Basisanschlusses permanent für andere Anwendungen (Telephon, Fax, Internet) verfügbar. Bei kleinen Datenpaketen (Kartenautorisierung, Alarmticket) ist eine auf 9,6 kbit/s reduzierte Übertragungsrate durchaus sinnvoll.

COMTESYS Sarl

Communication Models und Test Systems

Schweizer *TDT*-Partner bietet maßgeschneiderte Telekommunikationslösungen an.

Die Nähe zum Markt, das Wissen u m die Bedürfnisse der Kunden und die Lösungsfindung für künftige Telekommunikationsprojekte zeichnen einen erfolgreichen Unternehmer aus. Für die Schweiz hat sich Johann M. Hager, Geschäftsführer der Firma COMTESYS, zu einem wichtigen Partner entwickelt. Der 53-jährige Unternehmer, der den Schweizer Markt wie seine Westentasche kennt, plant mit dem niederbayerischen Unternehmen für schweizerische Firmen effektive und zukunftsorientierte Telekommunikationsprojekte. Das Verständnis für Lösungen konnte der passionierte Skifahrer, der in Genf lebt, in international tätigen Unternehmen erwerben. Seit einigen Jahren konzentriert sich der Ingenieur mit einem zusätzlich abgeschlossenen Wirtschaftsstudium auf die Telekommunikationsbranche. Die Projekte bespricht Johann M. Hager je nach Bedarf auf Deutsch, Englisch oder Französisch - und durch die Zusammenarbeit mit *TDT* kann er maßgeschneiderte Lösungen anbieten. Der Ausbau des ISDN-Netzes in der Schweiz und die *TDT*-Produktpalette, z. B. der DCC System 3 (Einwahlpool), NetMACS (Netzwerkmanagement-Software), Terminaladapter, MICRO Router, ALPHA Router und sämtliche OEM-Versionen eröffnet vielen Unternehmen neue, effektivere Kommunikationswege. Als Systemanbieter kann COMTESYS zum Beispiel für sämtliche Finanztransaktionen über das öffentliche Kommunikationsnetz oder TCP/IP in der Praxis erprobte Modelle anbieten. Dabei kann es sich um Kreditkartenautorisierungen, Sperrlistenübertragungen oder um die Einlieferung von durch Cash-Karten bezahlte Beträge handeln. Neben den bereits bewährten Einsätzen von *TDT*-Geräten werden Integratoren von Kartenlesegeräten künftig vermehrt auf Fernwartung bauen. „Dies trifft besonders für Maschinen- und Automatenhersteller jeglicher Art zu: Ein Billettautomat, ein Getränkeautomat, eine Waschmaschine oder eine Tankstelle kann über die gleiche Kommunikationsschnittstelle zum Fest- oder Natelnetz, Karteninformationen übertragen und ferngewartet werden. NetMACS, die Netzwerkmanagement-Software von *TDT*, ermöglicht Fernwartung, Fernkonfiguration und Software-Download sowohl für das Kommunikationsgerät als auch für den angeschlossenen Automaten”, so Johann M. Hager in einem Gespräch über die künftigen Einsatzmöglichkeiten für Maschinenhersteller. Dabei betont er, dass dies nicht nur für die großen Unternehmen gilt, sondern dass vor allem auch mittelständische Unternehmen erhebliche Kosteneinsparungen erzielen können. Regelmäßige Arbeitstreffen im Hause *TDT* und die Erfahrung der letzten Jahre sind die Garantie für eine fundierte Beratung und zufriedene Kunden in der Schweiz.

Kryptographie

Z A A S G W L P U M G K

TEIL 2

Das Vigenère-Verfahren

Ein besserer Ansatz ist das Vigenère-Verfahren. Es basiert darauf, dass für die einzelnen Buchstaben des Klartextes zum Verschlüsseln nicht dieselbe, sondern mehrere verschiedene monoalphabetische Verschlüsselungen verwendet werden und geht auf den „französischen Diplomaten Blaise de Vigenère (1523 bis 1596)“ zurück. Der Schlüssel ist dann nicht mehr, wie bei der Cäsar-Verschlüsselung, der Buchstabe, mit dem das verschobene Alphabet beginnt (s.o.), sondern ein Wort, wobei jeder Buchstabe des Schlüsselwortes für eine Cäsar-Verschlüsselung steht. Lautet das Schlüsselwort beispielsweise GESICHRT, so ergeben sich 8 verschiedene Cäsar-Verschlüsselungen, die rotierend auf den Test angewandt werden. Lautet der zu verschlüsselnde Text „Dieser Text wurde gegen unbefugtes Lesen gesichert“, ergibt sich:

Klartext:

DIESERTEXTWURDEGEGENUNBEFUGTESLESENGESICHERT
Schlüsselbuchst.:

GESICHRTGESICHRTGESICHRTGESICHRTGESICHRTGESI

Es ergibt sich also, abhängig von der Position des Klartextbuchstabens, eine jeweils andere Cäsar-Verschlüsselung. Auch entspricht die statistische Buchstabenverteilung des verschlüsselten Textes keiner Charakteristik mehr, so dass die Zuordnung der Geheimsymbole zu den Klartextsymbolen nicht so einfach wie bei der monoalphabetischen Substitution möglich ist.

Ist jedoch die Schlüssellänge bekannt, lässt sich die Vigenère-Verschlüsselung bei der Analyse eines Geheimtextes auf Cäsar-Verschlüsselungen zurückführen, da der Schlüssel ja periodisch wiederholt wird. Betrachtet man also jedes Zeichen, das mit dem gleichen Schlüsselbuchstaben verschlüsselt wurde (in unserem Beispiel also jedes 8. Zeichen), so gehorchen diese Geheimzeichen wieder der gleichen Häufigkeitsverteilung wie bei der monoalphabetischen Substitution. Die Schlüssellänge lässt sich mit geeigneten statistischen Verfahren leicht bestimmen.

Obwohl diese Unsicherheit des Vigenère-Algorithmus natürlich bekannt ist, wird er sogar in moderner Software noch eingesetzt, zum Beispiel bei der Textverarbeitung WordPerfect. Dies zeigt, wie wenig man sich auf diese Art von Verschlüsselung verlassen kann. Zum Glück gibt es für wichtige Daten natürlich auch Alternativen, wie die modernen Algorithmen zeigen, aber dazu später.

Das One-Time-Pad

Ist allerdings der Schlüssel annähernd so lang wie der Text, der verschlüsselt werden soll, lassen sich auf diese Art und Weise natürlich keine Gesetzmäßigkeiten mehr feststellen, da man dann ja keine Buchstabengruppe mehr erhält, die mit dem gleichen Schlüsselbuchstaben verschlüsselt worden ist! Diesem Verfahren kommt in der Kryptologie eine Sonderrolle zu: Es ist das einzige Verfahren, das sogar mathematisch beweisbar sicher ist, allerdings nur so lange, wie als Schlüsselbuchstaben eine rein zufällige Buchstabenfolge verwendet wird, die absolut keiner Gesetzmäßigkeit mehr gehorcht. Diese besondere Art der polyalphabetischen Substitution wird auch als „One-Time-Pad“ bezeichnet.

Da ein solcher Schlüssel natürlich nicht leicht übermittelt werden kann, ist dies auch das größte Problem dieses Verfahrens. Man könnte natürlich auf die Idee kommen, ein literarisches Werk als Schlüssel zu verwenden, die nötige Information zum Rekonstruieren der Nachricht könnte dem Empfänger leicht übermittelt werden, er braucht sich dann nur das entsprechende Werk zu besorgen. Allerdings ist die Folge von Schlüsselbuchstaben dann natürlich nicht mehr zufällig, sondern gehorcht den selben statistischen Verteilungen, die wir uns schon beim Knacken der monoalphabetischen Substitution zunutze gemacht haben. Also ist in diesem Fall keine Sicherheit mehr gewährleistet. Abwandlungen des One-Time-Pad-Verfahrens werden manchmal auch in modernen Verschlüsselungsprogrammen verwendet. Zur Schlüsselgenerierung wird dann eine Pseudo-Zufallszahlenfolge verwendet. Die Qualität des Verfahrens hängt dann im Wesentlichen von der Qualität der generierten Zahlenfolge ab.

Moderne Verschlüsselungsalgorithmen

Von den bisher besprochenen Verschlüsselungsalgorithmen sind wegen der beschriebenen Unsicherheiten nur noch Varianten des One-Time-Pad, und leider trotz der bekannten Unsicherheit auch des Vigenère-Verfahrens, im Gebrauch. Daher sollen im Folgenden einige moderne Verfahren kurz genannt werden. Die Beschreibung kann jedoch nicht so ausführlich wie bei den einfachen Verfahren sein, da die modernen Algorithmen meist sehr viel komplexer sind und einige Mathematik voraussetzen.

Feistel-Netzwerke (DES)

Anfang der 70er Jahre wurde von dem IBM-Mitarbeiter Horst Feistel das Konzept der Feistel-Netzwerke veröffentlicht, die die Basis für viele moderne Verfahren bildet, darunter auch das vor allem im Bankwesen sehr gebräuchliche DES (Data Encryption Standard). Im Gegensatz zu den bisher besprochenen Algorithmen, bei denen es sich um sogenannte Stromchiffren handelte, sind die Feistel-Netzwerke sogenannte Blockchiffren. Das bedeutet, dass der Klartext zunächst in gleichlange Blöcke geteilt werden muss, die dann durch den Algorithmus in ebenfalls gleich lange Geheimtextblöcke überführt werden. Bei den Feistel-Netzwerken wird zunächst der Klartextblock in zwei gleichgroße Halbblöcke geteilt und in zwei neue Halbblöcke überführt. Als neuer linker Block wird der alte rechte Halbblock genommen, zur Berechnung des neuen rechten Halbblocks wird der alte rechte Halbblock mit einer Funktion f, die sich aus dem Schlüssel und einem veränderlichen Rundenschlüssel ergibt, verschlüsselt und anschließend mit dem alten linken Halbblock bitweise Exklusiv-Oder verknüpft. Dies wird nun mehrmals, jeweils von den neuen, sich
ergebenden Halbblöcken ausgehend, mit verschiedenen Rundenschlüsseln wiederholt. Ein solcher Durchlauf heißt auch eine Runde.
Die Besonderheit dieses Verfahrens besteht darin, dass man mittels Umformungen der sich daraus ergebenden Gleichungen die Geheimtexte dechiffrieren kann, ohne dass die Funktion f umkehrbar sein muss. Wie schon erwähnt, ist der DES-Algorithmus ein solches Feistel-Netzwerk und „verwendet einen 56 Bit langen Schlüssel, um blockweise 64 Bit Klartext in 64 Bit Geheimtext zu überführen bzw. umgekehrt. Das geschieht in 16 schlüsselabhängigen Runden“.
Anwendungsgebiete von DES sind neben dem Bankwesen z.B. auch die Paßwortverschlüsselung bei Unix-Systemen. Zwar gilt der DES-Algorithmus immer noch als sehr sicher, jedoch sind bestimmte Angriffe, die meistens auf ein systematisches Durchprobieren aller möglicher 256 Schlüssel hinauslaufen, nicht ausgeschlossen. Diese Angriffe haben alle gemeinsam, dass sie nur mit sehr großem Aufwand an Hardware und Zeit realisiert werden können. Eine mit DES verschlüsselte Chiffre könnte daher möglicherweise, wenn man berücksichtigt, dass das Brechen des Codes auch als Dienstleistung angeboten werden könnte, schon unter Aufwand einer „fünf- oder sechsstelligen Summe“ geknackt werden.

Asymmetrische Verfahren

Die bisher betrachteten Verfahren sind zwar teilweise sehr sicher, sie haben aber alle das Problem der Schlüsselübermittlung gemeinsam: Sowohl der Sender als auch der Empfänger benötigen einen geheimen Schlüssel, der vorher auf einem sicheren Weg übertragen werden muss. Weil derselbe Schlüssel sowohl zum Chiffrieren als auch zum Dechiffrieren verwendet wird, spricht man auch von symmetrischen Verfahren. Eine Lösung dieses Problems bieten jedoch die neuen, asymmetrischen Verfahren. Hierbei findet sowohl ein geheimer als auch ein öffentlicher Schlüssel Verwendung. Der geheime Schlüssel kann aus dem öffentlichen Schlüssel nicht hergeleitet werden. Da hierbei die Problematik des Schlüsselaustausches wegfällt, wird diese Art der Chiffrierung heute sehr oft für E-Mails angewandt.

Will eine Person A einer Person B eine verschlüsselte Nachricht zukommen lassen, so benötigt A zunächst den öffentlichen Schlüssel von B. Dieser kann von B gefahrlos bekannt gegeben werden, da er nur zum Verschlüsseln dient, nicht aber zum Entschlüsseln. Hierfür benutzt B den geheimen Schlüssel, der von B unter Verschluss gehalten wird. Einige asymmetrische Verfahren, darunter das bekannte RSA, ermöglichen darüber hinaus die Erstellung von so genannten digitalen Unterschriften. Hierbei wird das Verfahren einfach „umgekehrt“ angewandt: Der geheime Schlüssel wird zum Chiffrieren verwendet, und die erhaltene Nachricht kann dann mit dem öffentlichen Schlüssel dechiffriert werden. Damit gilt also jede Nachricht, die mit einem öffentlichen
Schlüssel dechiffriert werden kann, als authentisch, da sie mit dem geheimen Schlüssel, der unter Verschluss ist, verschlüsselt worden sein muß.

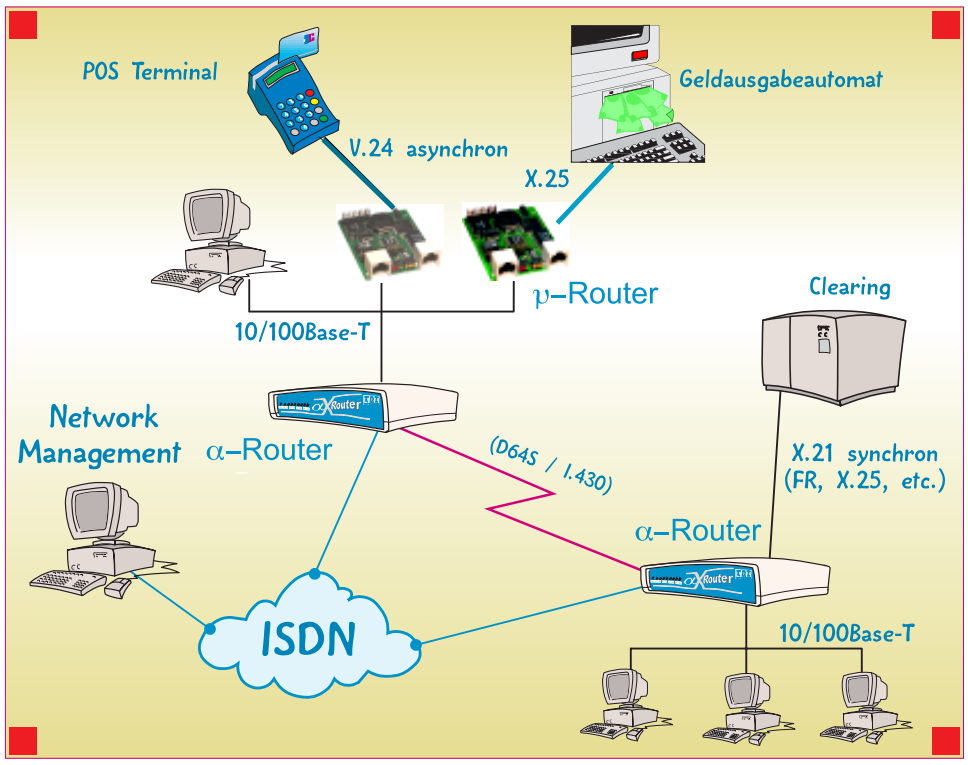
Obwohl das Verfahren zu komplex ist, als dass man es hier in Kürze beschreiben könnte, soll wenigstens der Ansatz des wohl populärsten asymmetrischen Algorithmus, des RSA-Algorithmus, der unter anderem in dem bekannten Programm PGP verwendet wird, kurz gezeigt werden: Möglich wird ein solches Verfahren durch die mathematischen Probleme des diskreten Logarithmus, also die nach x aufgelöste Form einer Gleichung der Form ax = g mod n. Da wir hier Modulo, also ganzzahlig mit Rest, rechnen, ist die Lösung nicht etwa loga(g), sondern insbesondere für große n sehr schwierig herzuleiten. Des Weiteren spielt das Problem der Faktorisierung großer Zahlen der Form p*q, p und q seien Primzahlen, eine Rolle. Für große Zahlen ist dies nämlich mit einem sehr hohen Aufwand verbunden; im RSA-Algorithmus wird hiermit das Herleiten des geheimen aus dem öffentlichen Schlüssel erschwert. Der RSA-Algorithmus wäre also gebrochen, wenn man ein einfaches Verfahren zur Faktorisierung großer Zahlen finden würde.

Nachteile des RSA-Verfahrens sind der hohe Zeitaufwand für das Chiffrieren und Dechiffrieren sowie die leichte Angreifbarkeit, wenn Teile des Klartextes bekannt sind. Daher wird es in gängiger Software wie z.B. PGP nur verwendet, um einen zufällig generierten und nur für eine Übermittlung benutzten „Sitzungsschlüssel“ für ein symmetrisches Verfahren zu chiffrieren, mit dem der eigentliche Klartext chiffriert wird. Da der Sitzungsschlüssel selbst mit einem sicheren Verfahren verschlüsselt ist, kann er dann gefahrlos zusammen mit der mit dem symmetrischen Verfahren chiffrierten Botschaft übermittelt werden.

Die Verwendung von asymmetrischen Verschlüsselungsalgorithmen erleichtert zwar den Schlüsselaustausch, da ein Teil des Schlüssel ja öffentlich ist und nicht geheim gehalten zu werden braucht, da diese Algorithmen jedoch gerade bei E-Mail-Kontakten angewandt werden, bei der sich die Kommunikationspartner unter Umständen noch nie persönlich begegnet sind, ergibt sich die Fragestellung, ob derjenige, von dem wir den öffentlichen Schlüssel erhalten haben, auch derjenige ist, der er zu sein vorgibt. Ein potentieller Angreifer könnte beispielsweise den E-Mail-Verkehr zwischen zwei Benutzern abfangen, und beiden gefälschte öffentliche Schlüssel zuspielen, indem er vorgibt, der jeweils andere Kommunikationspartner zu sein. Jedoch lässt sich auch diese Gefahr durch geeignete Verfahren minimieren, worauf allerdings nicht näher eingegangen werden soll.

T.D.T.-APPLIKATIONEN

für MICRO- und ALPHA-Router



MICRO-Router von T.D.T.

Der MICRO-Router ist eine schlüsselfertige Lösung für OEMs, die ein vorhandenes oder geplantes Produkt mit dem Intra- oder Internet verbinden wollen. Die *TDT*-Entwicklung besitzt eine 10Base-T-Ethernet- und eine ISDN BRI-Schnittstelle. Anwenderseitig wird das kleine System über eine serielle asynchrone oder synchrone Schnittstelle (V.24/V.28 oder TTL) angesprochen. Eine zweite Schnittstelle mit TTL-Pegel steht als Option zur Verfügung. Damit lassen sich alle Geräte direkt oder indirekt über das ISDN-Netz an ein LAN koppeln.
Das Gerät besitzt neben den üblichen Routingfunktionen integrierte IP/ISDN-, IP/FR- und IP/X.25-Gateway Module, mittels denen sich IP-Daten über ein ISDN-, Frame Relay- oder X.25-Netz weitervermitteln lassen. Es können zusätzliche Anwender-Protokolle implementiert werden, um „dumme Endgeräte" IP-fähig zu machen. Die Einsatzmöglichkeiten sind vielfältig, z. B.:

- ★ Steuerung und Überwachung von industriellen Prozessen jeder Art
- ★ Druckereimaschinen
- ★ Wetterstationen
- ★ POS-Terminal Cluster per LAN
- ★ Fernwartung und Gebührenerfassung
- ★ Erfassung von Verbrauchsdaten
- ★ Aufzugsysteme
- ★ Gebäudetechnik usw.

Neues Feature im ALPHA-Router und MICRO-Router, XOT und Gateway

Wohl einmalig ist das Feature XOT und Gateway in einem Router dieser Preisklasse. Mit XOT läßt sich X.25 in TCP übertragen. Das Besondere daran ist, dass es sich hier nicht um ein einfaches "tunneling" handelt. Die gesicherte Übertragung, die normalerweise von der Ebene II (HDLC) bei X.25 übernommen wird, kann wegfallen. TCP übernimmt diese Aufgabe.
Die Gateway-Funktionalität im ALPHA Router ist vielfältig. Es können z.B. X.25-Daten die via TCP/IP angeliefert werden auf Basis der IP-Nummer oder der X.25-Rufnummer über eine beliebige ISDN-Nummer weitervermittelt werden. Zusätzlich kann die rufende als auch gerufene X.25-Nummer verändert werden, einschließlich des User Data Fields und des Facility Fields. Die Möglichkeiten der Gateway-Funktion sind sehr vielseitig - es lohnt sich ein Anruf bei *TDT*.

Jetzt schon vormerken:
SYSTEMS in München
6.–10. November 2000

T.D.T.-EVENT 2000

Firmeninhaber Michael Pickhardt heiratet Sabine Laermann

Eine rauschende Hochzeitsfeier mit vielen Überraschungsmomenten bereiteten Verwandte und Freunde dem frisch vermählten Paar Pickhardt.

Foto links: Die Feuerwehr stand auf sehr originelle Weise Spalier.

Foto links unten:
Die Darsteller der Landshuter Fürstenhochzeit überraschten mit musikalischen Glückwünschen vor dem Standesamt Essenbach.

Foto unten:
Sabine und Michael Pickhardt genossen sichtlich die Darbietung der Künstler.

Jürgen Siegl neuer stellvertretender Produktionsleiter

Zuverlässige, schnelle Arbeit ist der „Feuerwehrmann" aus Altheim gewohnt. Diese Eigenschaften setzt Jürgen Siegl auch in seiner täglichen Arbeit als stellvertretender *TDT*-Produktionsleiter ein. Zusammen mit Produktionsleiterin Maria Mayer ist er für die Koordinierung und Überwachung der Produktion laut dem QM-System nach DIN EN ISO 9001 verantwortlich.

24-Stunden-Support-Service

Eines ist klar: Der Ausfall oder die Unterbrechung von Datenübertragungen kommt immer gerade zum ungünstigsten Zeitpunkt. *TDT* hat deshalb den Support-Service auf 24 Stunden ausgedehnt. Weitere Infos erhalten Sie unter Tel. 0 87 03/9 29-200

Editorial

Nun wissen wir es! Deutschland steht nicht auf der Wunschliste indischer Computerspezialisten. Dabei spielt es keine Rolle, welche Karte wir ihnen zu geben gedenken. Talentierte ausländische Fachkräfte zieht es noch immer in die USA. Deutschland, und das nicht erst seit dem Ausscheiden bei der Fußball-Euro, verliert international an Stellenwert. Doch jede Medaille hat bekanntlich zwei Seiten. Für *TDT* kann ich aus eigener Erfahrung bestätigen, dass in der Aus- und Weiterbildung schon immer unkonventionelle Wege gegangen worden sind. Viele meiner Kollegen sind Quereinsteiger, denn *TDT* hat Ihnen die Möglichkeit gegeben, sich in einem völlig neuen Berufsbild einarbeiten zu können. Den Nutzen davon haben beide Seiten - und unsere Kunden.

Herzlichst Ihr Max Hendlmeier

OEM-Versionen der Terminaladapter von T.D.T. immer beliebter

Mehr als hundert verschiedene Software-Versionen bereits im Einsatz

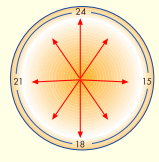
Maschinenhersteller aller Couleur setzen auf TA-OEM-Versionen, um die Anbindung ihrer Geräte und Maschinen an das ISDN-Netz preisgünstig lösen zu können. So kommt es nicht von ungefähr, dass gerade nachdem der erste Prototyp der 9. Hardware-Variante hergestellt worden ist, bereits am Design für die Hardware-Serie Nr. 10 gearbeitet wird.

Weltweite Knappheit für Bauteile

Elementare Bauteile sind zurzeit weltweit so gut wie vergriffen

Deswegen kann es schon mal vorkommen, dass Geräte nicht fertiggebaut werden, weil ein bestimmtes Bauteil zur Zeit einfach nicht geliefert werden kann.
***TDT* hat schon im Vorfeld reagiert und genügend Vorrat für die gefährdeten Teile geordert.**

Weitere Infos zu der aktuellen Situation gibt Ihnen gerne Maria Mayer.



T.D.T.-Geräteschulung

Jetzt für Herbst anmelden

Die nächste Geräte- und Protokoll-Schulung wird voraussichtlich am 24./25. Oktober 2000 stattfinden.
Kontaktieren Sie uns bitte via

E-Mail info@tdt.de
Telefon 0 87 03/9 29-00
Fax 0 87 03/9 29-2 01

Gerne geben wir Ihnen weitere detaillierte Infos.

IMPRESSUM

Herausgeber	T.D.T. Transfer Data Test GmbH Siemensstraße 18 84051 Essenbach Tel. 08703/9 29-00 Fax 08703/9 29-201 E-Mail info@tdt.de http:///www.tdt.de
Verantwortlich für den Inhalt	Michael Pickhardt, Geschäftsführer H. J. Büttner
Gesamt produktion	Werbeagentur J. Wimmer Ulmenstraße 21 84051 Essenbach Tel. 0 87 03/9 13 60 Fax 0 87 03/9 13 61
Auflage:	28.000 Exemplare
Ausgabe 2/00	Auf Umweltpapier gedruckt