SIRAGA 321 - **modernste Chiffriertechnologie für die**

Sicherung Ihrer vertraulichen und geheimen
Internet - Telefonate

gegen Mithören und Mißbrauch durch Jedermann

Mit den Siraga 321 – Crypto-Vorsatzgeräten für INTERNET - Telefonate aller Modifikationen schuf das Ingenieurbüro für NachrichtenSicherheit Berlin eine Systemkomponente , welche Ihre Telefonate im INTERNET wirkungsvoll und auf der Grundlage echter Zufallsfolgen *zuverlässig gegenüber allen unberechtigten Mithörversuchen sichert.*
Der unberechtigte Angreifer hat keine Chanche , nur Ihr Gesprächspartner kann , geschützt vor fremden Ohren, Ihre Stimme hören . Genauso können nur Sie die Stimme Ihres Gesprächspartners verstehen.

Sehen Sie das grüne Signal oder im Display das Wort „ SICHER „ dann arbeitet Ihr hochsicherer Chiffrierkanal.

Die Verkehrsmethode ist eine individuelle, semiduplexe, Ende-zu-Ende Telefonie-Chiffrierverbindung, bei welcher nur die beiden Nutzer , Sie und Ihr Partner einen ca. 20 stelligen , mit einem echten Zufallsgenerator ermittelten, Tagesschlüssel oder Sitzungsschlüssel kennen. Auf Wunsch werden Schlüsselunterlagen im Beisein der Nutzer erstellt.

Die Chiffriermethode ist die Blockchiffrierung durch Transposition, bei Geräten der garantierten Sicherheit die OTP Methode.
Zur unberechtigten Dechiffrierung durch jeden Angreifer müssen ca. 10^{200} Möglichkeiten der Zuordnung der einige ms -langen Sprachfetzen für jeden Block durchgerechnet werde. Selbst wenn die heutigen Computerkapazitäten mit 1000.000 multipliziert würden , würde es durchschnittlich Jahrhunderte dauern, um zum Klartext vorzudringen.

Das System :
Mit dem SIRAGA 311 können Sie mit allen SIRAGA 3.. Geräten Ihrer Gesprächspartner (SIRAGA - 31* für Festnetzverbindungen, - 32* für Internettelefonie über SKYPE u.ä. Systeme , - 33* für GSM- Funktelefone sowie SIRAGA – 34* für Satellitenverbindungen Verbindung aufnehmen und unabhängig vom Übertragungskanal zum Partner hochsichere Sprachverbindungen betreiben , in denen Sie mit Ihrem Partner sicher und ohne unberechtigte Lauscher kommunizieren können.
Ist Ihr Gesprächspartner über ein analoges Funkgerät an das öffentliche Netz angeschaltet (z.B. über Überleiteinrichtungen / Seefunk) kann dieser mit Ihnen über SIRAGA 35* für analoge Funkgeräte sicher kommunizieren.

Das SIRAGA 321 ohne Benutzerführung beispielsweise mit Handapparat

Das SIRAGA 321 mit Benutzerführung beispielsweise mit Sprechgarnitur

Die Benutzung :

Das Sprachchiffriergerät wird an die Anschlüsse der Audiokarte des Computers angeschlossen , die Spannungsversorgung wird eingesteckt und die „ normale „ Internet- Sprachverbindung (VOIP) hergestellt.
Wird eine verschlüsselte Verbindung gewünscht, stellen die Teilnehmer mit der Matrix den entsprechenden Tages- oder Sitzungsschlüssel ein, schalten das Crypto – Vorsatzgerät auf „ sicherer Verkehr „ und telefonieren nun , nachdem sie sich überzeugt haben , daß die große grüne LED leuchtet , über die am Crypto – Vorsatzgerät angeschaltete Sicherheits- Hör-Sprech- Garnitur oder den Handapparat.
Durch das Drücken der Sprechtaste wird der Sprechkanal geschaltet. Nach dem Loslassen hören Sie mit einer Verzögerung von ca. 3 Sekunden die entschlüsselte Sprache Ihres Partners.
Sie haben damit einen eigenen Telefonkanal zu Ihrem Telekommunikations-partner , in den n i e m a n d eindringen kann, der nicht den Schlüssel besitzt.

SIRAGA 311 können Sie als SIRAGA 311 A in der Normalausführung mit Schlüsseleinstellmatrix , als SIRAGA 311 B (B wie Benutzerführung) mit Schlüsseleinstellmatrix und Display oder als SIRAGA 311C , wie 311 A , jedoch mit garantierter Sicherheit, erwerben.

SIRAGA 321 sicherste Internet-Telefonie

Klasse	Permutationen	Schlüsselraum
 Höchste Sicherheit „ A „	ca. 10^{200}	ca.10^{20}
 Garantierte Sicherheit „ C „		OTP

Herausragende Qualitätsmerkmale der Geräte :

Höchste Sicherheit durch symmetrische Chiffrierung
Die an jeden beliebigen Kanal anschließbaren Geräte stellen zwischen den berechtigten Teilnehmern eine durchgängige Ende zu Ende Chiffrierung , also vom Mund des Sprechenden bis zum Ohr des Hörenden , her.
Ob Festnetz- oder GSM- Telefonie, VOIP , Satelliten- oder Funkkanäle , die Gesprächsinhalte werden zu einem Analogsignal verarbeitet, bei dem auch der bestausgestattetste unberechtigte Lauscher zunächst jahrzehntelang ca.10 200 Möglichkeiten durchprobieren muß, um an einen sekundenlangen Gesprächsfetzen zu gelangen. Selbst der Supercomputer Jüllich hätte damit seine arge Not.

Vollständige Schlüsselherrschaft über echten Zufallsschlüssel
Nicht irgendwelche unkontrollierbar - anonymen Schlüsselserver sondern *ausschließlich die berechtigten Teilnehmer verfügen über die Schlüssel*, die zur Erhöhung der Sicherheit von ihnen sogar spontan individuell verändert werden können.
Die Inertialschlüssel entspringen einem *echten , physikalischen Zufallsprozeß*.
Da Schlüsseldaten unmittelbar nach Gebrauch sicher gelöscht werden (ähnliches Verfahren wie z.B. VS-Clean), besteht während des Gespräches und nach Gesprächsschluß keine Möglichkeit , Schlüsseldaten zur unberechtigten Kenntnisnahme, etwa durch Kanalmitschnitte, zu ermitteln.

Sicherheit für jeden Zweck
SIRAGA´s der hohen Sicherheit schützen sicher vor Angriffsversuchen von freaks , vor Zufallserfolgen von im Übertragungssystem arbeitenden Mitarbeitern und anderen unberechtigten Dritten , die nicht über Großrechentechnik verfügen.
Die Gesprächsanalyse über Schlüsselwörter und Wortdatenbanken ist ausgeschlossen.
SIRAGA´s der höchsten Sicherheit schützen sicher vor Angriffsversuchen, bei denen Angreifer über Großrechenanlagen verfügen.
SIRAGA´s der garantierten Sicherheit werden auf Anfrage hergestellt.
Über die, mit der zweifelsfrei unknackbaren OTP- Methode arbeitenden, Geräte können Gespräche mit den höchsten Geheimhaltungsanforderungen geführt werden.
Die Gesprächsanalyse über Schlüsselwörter und Wortdatenbanken ist ausgeschlossen.

Keine demaskierenden Prozeßdaten
Weder über die ungesicherte noch über die chiffrierte Verbindung werden irgendwelche Schlüssel , Teile von Schlüsseln, Derivate oder andere enttarnende Regieanweisungen übermittelt , die es dem unberechtigten Lauscher erleichtern würden, mit großen Rechnerkapazitäten nach absehbarer Zeit in die Verbindung einzudringen. Demaskierende Abstrahlungen wurden nicht festgestellt , so daß Tempest Angriffe auch in Zone 1 nicht zum Erfolg führen. Symmetrische Leitungsführungen zum Handapparat / Sprechgarnitur reduzieren auch hier mögliche Felder auf ein Minimum.

Software- oder Onlineangriffe unmöglich

Die Geräte sind hardwarebasiert, abstrahlungs- und sabotagegeschützt und **nicht Bestandteil von anderen , digital gekoppelten Systemelementen** wie Sat- oder GSM-Handys, Computern/ Netzwerkkomponenten oder ISDN Systemtelefonen. **Die analoge Kopplung** verhindert sicher ein elektronisches Eindringen in die und ein Manipulieren der Chiffriereinheit durch Schadsoftware oder fingierte Befehle.

Telefoniren Sie abhörsicher auf einem Niveau , das bisher nur Militärs und Behörden zugänglich war.

Schützen Sie Ihr Vermögen ,

Schützen Sie Ihre Geheimnisse

Schützen Sie Ihr Leben

Ingenieurbüro
für
NACHRICHTENSICHERHEIT
Oberstleutnant a.D. Dipl.- Ing
DIETER OSTMANN
D 12 679 Berlin , Blumberger Damm 168
Info@schnueffelschutz.de / www.schnueffelschutz.de