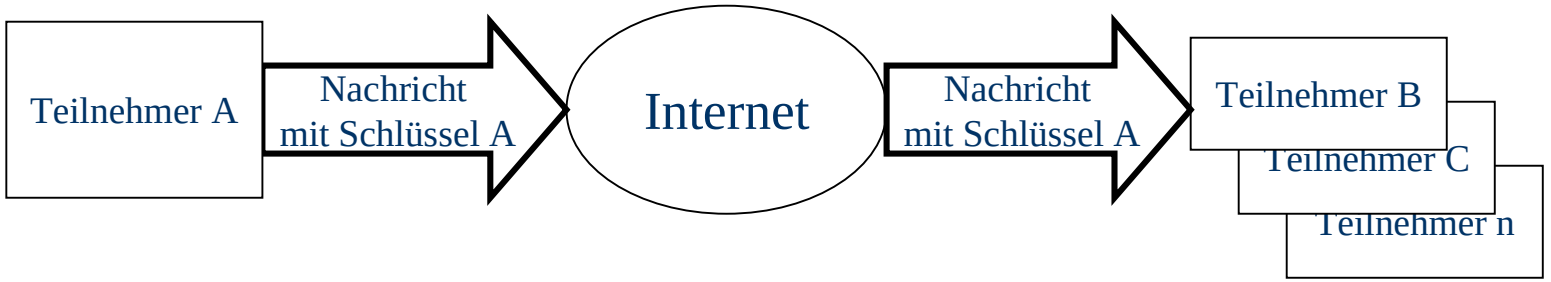
Intergramm –

Genial einfaches Verfahren zum Signieren und Verschlüsseln von Internet-Nachrichten

Symmetrische Verschlüsselung - klassisch



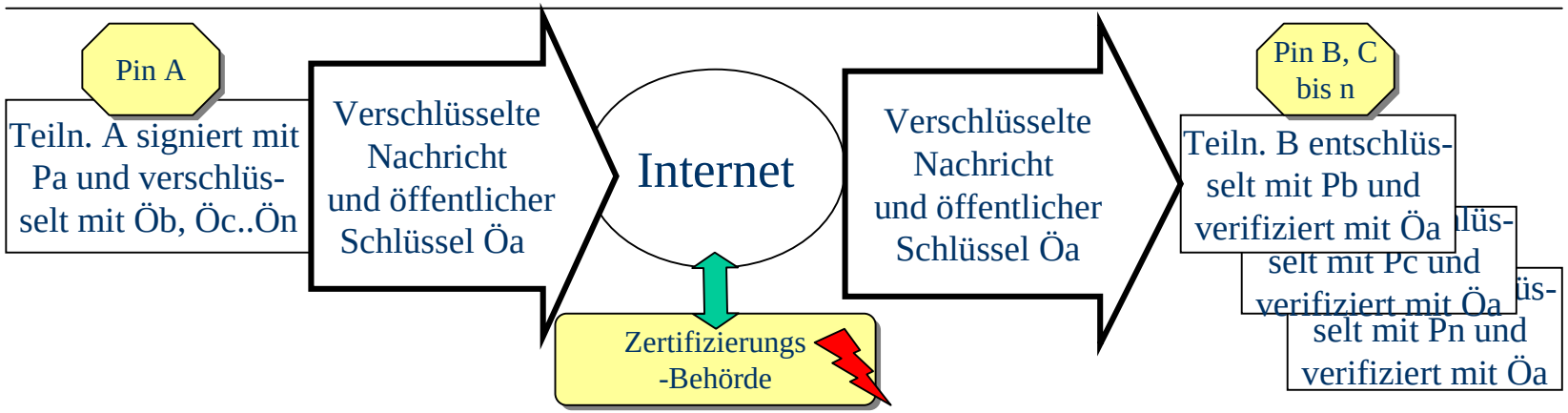
Vorgehensweise: Teilnehmer A verschlüsselt seine Nachricht mit dem Schlüssel A, sendet diese über das Internet an die gewünschten Teilnehmer B bis n, die die verschlüsselte Nachricht mit dem selben Schlüssel A entschlüsseln.

Vorteile: Einfache Verschlüsselung, einfache Handhabung, einfache Entschlüsselung

Nachteile: 1. Geringe Sicherheit, da die Geheimhaltung des Schlüssels bei steigender Anzahl der Teilnehmer sinkt. Auch deshalb müssen die Schlüssel regelmäßig geändert werden, d.h. hoher Betreuungsaufwand.
2. Keine eindeutige Identifizierung des Absenders möglich, da kein persönlicher Schlüssel benutzt wird.

Asymmetrische Verschlüsselung und Signierung

intergramm



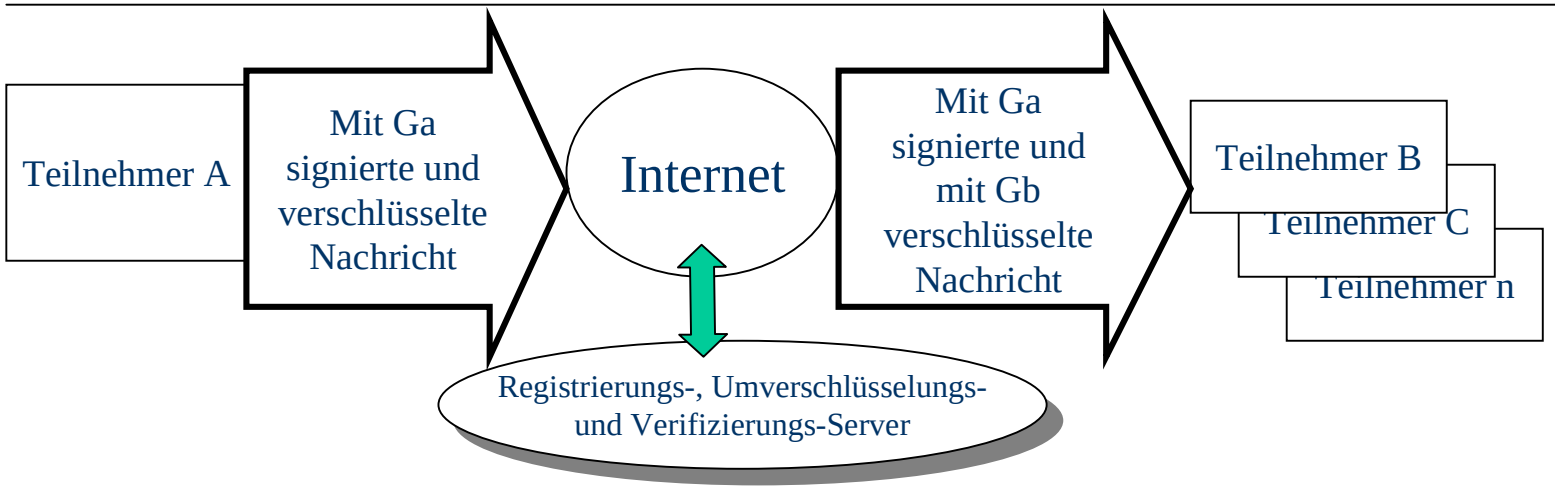
Vorgehensweise: Teilnehmer A erhält den Zugang zu seinem privaten Schlüssel Pa über seine Pin A. A signiert seine Nachricht mit Pa, verschlüsselt sie mit dem öffentlichen Schlüssel Öb des Teilnehmers B und sendet sie über das Internet an B. Gleichzeitig wird die Nachricht für alle weiteren Empfänger n mit deren öffentlichen Schlüsseln Ön verschlüsselt und versandt. Teilnehmer B erhält den Zugang zu seinem privaten Schlüssel Pb über seine Pin B. Er entschlüsselt die Nachricht mit Pb und verifiziert die Signatur mit dem öffentlichen Schlüssel Öa von A. Gleiches gilt für die anderen Teilnehmer C bis n.

Vorteile: Hohe Sicherheit, da jeder Teilnehmer sein eigenes Schlüsselpaar besitzt.

Nachteile:
1. Komplizierter, hoher und kostenintensiver Betreuungsaufwand bei Verwaltung der öffentlichen und persönlichen Schlüssel durch die Zertifizierungsbehörde. Dadurch keine Verbreitung trotz jahrelanger Vermarktung.
2. Signatur kompliziert und lang. Dadurch schwierige Wiedererkennung der Signatur.

Intergramm – die neue einfache und sichere Lösung

intergramm



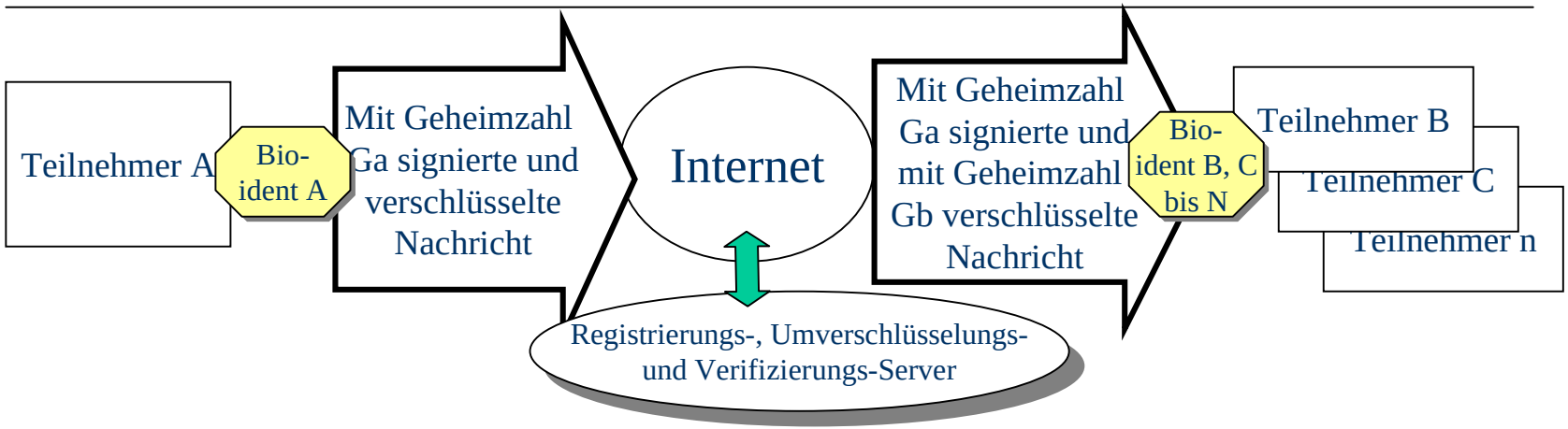
Vorgehensweise: Teilnehmer A signiert und verschlüsselt seine Nachricht mit seiner persönlichen Geheimzahl Ga. Die Nachricht wird über das Internet an den Registrierungs-Server gesendet, wo sie umverschlüsselt wird. Danach wird sie an den Teilnehmer B weitergesendet, der die Nachricht mit seiner eigenen Geheimzahl Gb entschlüsselt und die Signatur durch Kontakt mit dem Server verifiziert. Gleiches gilt für die Teilnehmer C bis n mit ihren jeweiligen Geheimzahlen Gc bis Gn.

Vorteile: Hohe Sicherheit, da jeder mit seiner eigenen persönlichen Geheimzahl G signiert und verschlüsselt. Einfache und kostengünstige Bedienung, da keine komplizierte formalisierte Registrierung nötig ist. Die Registrierung erfolgt über das Internet nach einer Identitätsprüfung des Teilnehmers. Signatur ist kurz und leicht zu erkennen.

Nachteile: keine

intergramm

Bio-ident: zusätzliche Sicherheit



Vorgehensweise: Teilnehmer A erhält die Berechtigung zur Aktivierung seiner Geheimzahl Ga über bio-ident. Bio-ident ist eine psychometrische Zugangsberechtigung und ersetzt den Pin-Code oder eine biometrische Eigentümlichkeit wie den Fingerabdruck. Bei bio-ident werden vom Teilnehmer vorab eingegebene Begriffspaare abgefragt. Die Signierung und Verschlüsselung der Nachricht findet mit der Geheimzahl Ga wie gehabt statt. Teilnehmer B aktiviert seine Geheimzahl Gb über sein eigenes bio-ident. Die Entschlüsselung und Verifizierung finden wie gehabt statt. Gleiches gilt für die Teilnehmer C bis n.

Vorteile: Der Teilnehmer muß sich keine PIN merken (hohe Vergeßlichkeitsrate; außerdem geringe Sicherheit, falls PIN aufgeschrieben wird). Die Begriffspaare von bio-ident (z.B. Vor- und Nachname von Jugendfreunden) kennt der Teilnehmer auswendig. Bei den üblichen biometrischen Verfahren (Iris-Scannen oder Fingerabdruck) besteht eine hohe Fehlerquote. Diese Verfahren können auch leicht getäuscht werden.

Nachteile: keine