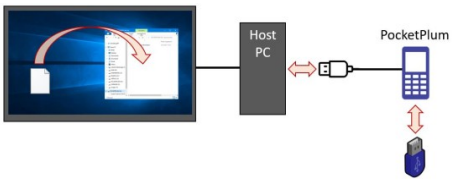
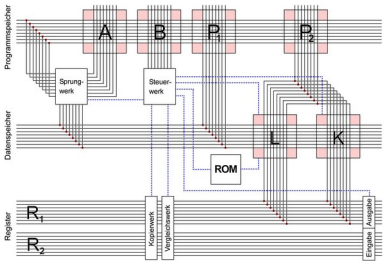
Neuromathematik ==> Assoziativtechnologie: *Vektografie und Assoziativmaschinen*, Unterschiede

1) Das Verfahren "Aplum". Hier liegt eine Assoziativmatrix im Kern der Prozesse, jedoch wird sie nicht gefüllt durch "Lernen" (von binären Frage-Antwort Paaren, wie üblich), sondern durch zufälliges bzw. pseudozufälliges Befüllen mit **1**en. Eine "Anfrage" wird nun durch diese Matrix völlig -aber rekonstruierbar- "verwirrt", was als Hilfsmittel für ein zu erzeugendes Chiffrat Verwendung findet. Wie die Parameter und die innewohnenden Falltürmechanismen in den einzelnen Modulen zu wählen sind, ist intensiv erforscht und geprüft. Dazu gehörten auch Ergebnisse der Standard-Tests der Statistik (NIST) für die iterierten Bitströme. Siehe imbit.net.



Das Verfahren (vom Typ Stream-Cipher) ist für zwei Anwendungen als Produkt verfügbar: (i) Für die Verschlüsselung einer **Datei** und (ii) als Transformationsmechanismus für einen Datenträger, wie z.B. einen **USB-Stick**. Beide Lösungen, sog. *Aplum-File* und *PocketPlum*, sind etwa zigarettenschachtelgroß, haben je einen eigenen Prozessor, ein Display mit Tastatur (oder Touch) und führen die Crypto-Transformationen unabhängig und ohne Hilfe eines Hostrechners durch. Im Unterschied zu anderen ist das "Plum"-Verfahren (beliebig) skalierbar, parallelisierbar und hat auch noch weitere "schöne" Eigenschaften, deren Erläuterung etwas mehr Zeit / Platz erforderte. Das jeweilige **Passwort liegt jedoch nicht auf dem Gerät** (auch kein Hash davon o.ä.), vielmehr setzt es den richtigen Prozess direkt in Gang - oder eben einen unbrauchbaren. Das trifft auf beide Varianten (i), (ii) zu. Architektur, Software und Prinzipien sind publiziert, ein Teil ist auf imbit.net einzusehen. Ein zugehöriges Patent ist mittlerweile offengelegt. Weil man am Bahngraphen der Transformations-Matrix die kryptografischen Eigenschaften sehr gut studieren kann, wurde die Basistechnik auch *Vektografie* genannt.

2) Assoziativmaschine (AM). Das ist eine Art Computer, aber ohne Rechenwerk und auch sonst von gänzlich anderer Architektur als der von-Neumann-Rechner. Im Kern besteht die Maschine aus mehreren Assoziativmatrizen, deren Prozesse und Zusammenarbeit völlig undurchsichtig sind. Ein Programm darin konstituiert sich aus der Art der **1**-Belegung der Matrizen. Und weil unterschiedliche Belegungen dennoch die gleiche Funktion realisieren können, sind sie resistent gegen Schadsoftware. (Es ist so ähnlich wie mit den Gehirnen: Zwei Schüler antworten beide korrekt auf die Aufgabe: Wieviel ist 5 mal 6? - obwohl sie verschiedene Zellen- und Synapsen-Verschaltungen im Gehirn haben.) Das Besondere für die Cybersicherheit liegt deshalb darin, dass die Assoziativmaschine zum Beispiel IoT-Anlagen -oder auch andere- betreiben und absichern kann, wobei Ausspähung oder manipulierte Beeinflussung nicht möglich ist. (Es ist so ähnlich wie beim Gehirn: Selbst wenn man es schichtenweise per CT durchscannt, weiß man nicht, was es gelernt hat - oder gerade denkt.) Die AM arbeitet ihre Programme auch noch zuverlässig ab, wenn äußere Einflüsse stören und Bits kippen (durch elektromagnetische oder ionisierende Strahlung o.ä.). Dank der innewohnenden Fehlertoleranz, d.h. Fähigkeiten zur Mustererkennung, kann eine Assoziativmaschine zudem eine sichere Zuordnung von z.B. schwankenden Sensordaten zu validen Merkmalen liefern, die dann in den externen Bereich übertragen werden (oder vor Ort eine Aktion auslösen). Wir haben das alles geprüft und getestet, jahrelang auch in unseren Masterkursen an der Universität unterrichtet und könnten das natürlich erläutern und anhand unserer Simulation "System 9" auch vorführen. Die eigens entwickelte Programmiersprache *VidAs 5* alias *am1prime* findet man (samt Beispielen usw.) in unserem Buch *Neuromathematik und Assoziativmaschinen*, Springer Vlg. 2013.



Zusätzliche Sicherheit auf den Übertragungswegen zwischen mehreren Assoziativmaschinen können Verschlüsselungsgeräte der Art Aplum schaffen, deren Wirkung ebenfalls auf Assoziativmatrizen-Technologie beruht und oben skizziert wurde.

Ende *Vektografie und Assoziativmaschinen*