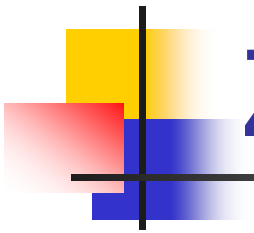
Distributed Computing And Cracking

Informatik-Seminar 2

Michael R. Albertin

Betreuer: Prof. Dr. P. Heinzmann

Cobetreuer: Prof. Dr. A. Rinkel



Ziel

- Sie kennen die Grundlagen zum verteilten Rechnen
- Sie verstehen, wie komplexe Aufgaben verteilt werden können
- Sie verstehen speziell, wie Distributed Cracking funktioniert

daraufhin ...
...werden Sie Ihr Leben ändern!

Einführung Grundlagen

- Rechenleistung in den letzten Jahren stark gestiegen
- Trotzdem: viele Aufgaben sind zu rechenintensiv

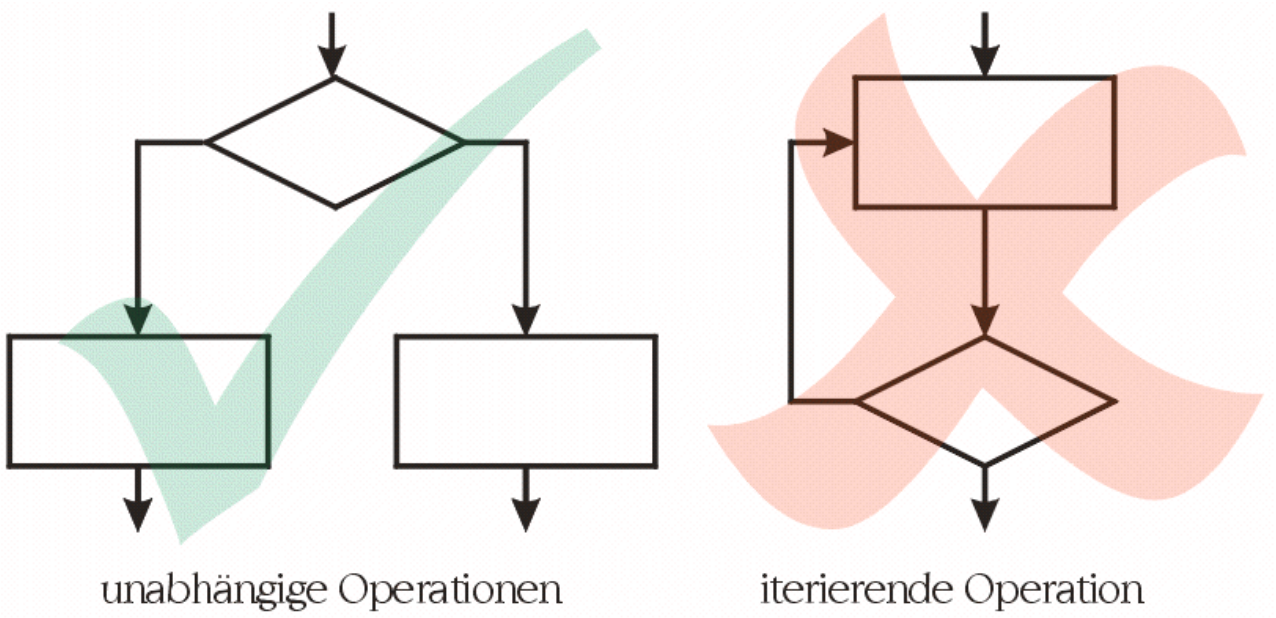
- Verschlüsselung nur sicher, solange keine einfache Crackmethode bekannt
- Crackmethode „BruteForce" funktioniert immer
- ist aber sehr zeitintensiv

Schlüssel	56bit	64bit	128bit	512bit
Anzahl Bit	56	64	128	512
Anz. Möglichkeiten	7.20576E+16	1.84467E+19	3.40282E+38	1.3408E+154
Dauer in Jahren	538	137878	2.5E+24	1E+140

- Berechnung aufteilen und an mehrere PCs verteilen

Einführung Voraussetzungen

- Voraussetzungen für Distr. Computing and Cracking
  - Aufgabe muss parallelisierbar sein
  - Verwaltungsaufwand darf Zeitgewinn nicht übersteigen

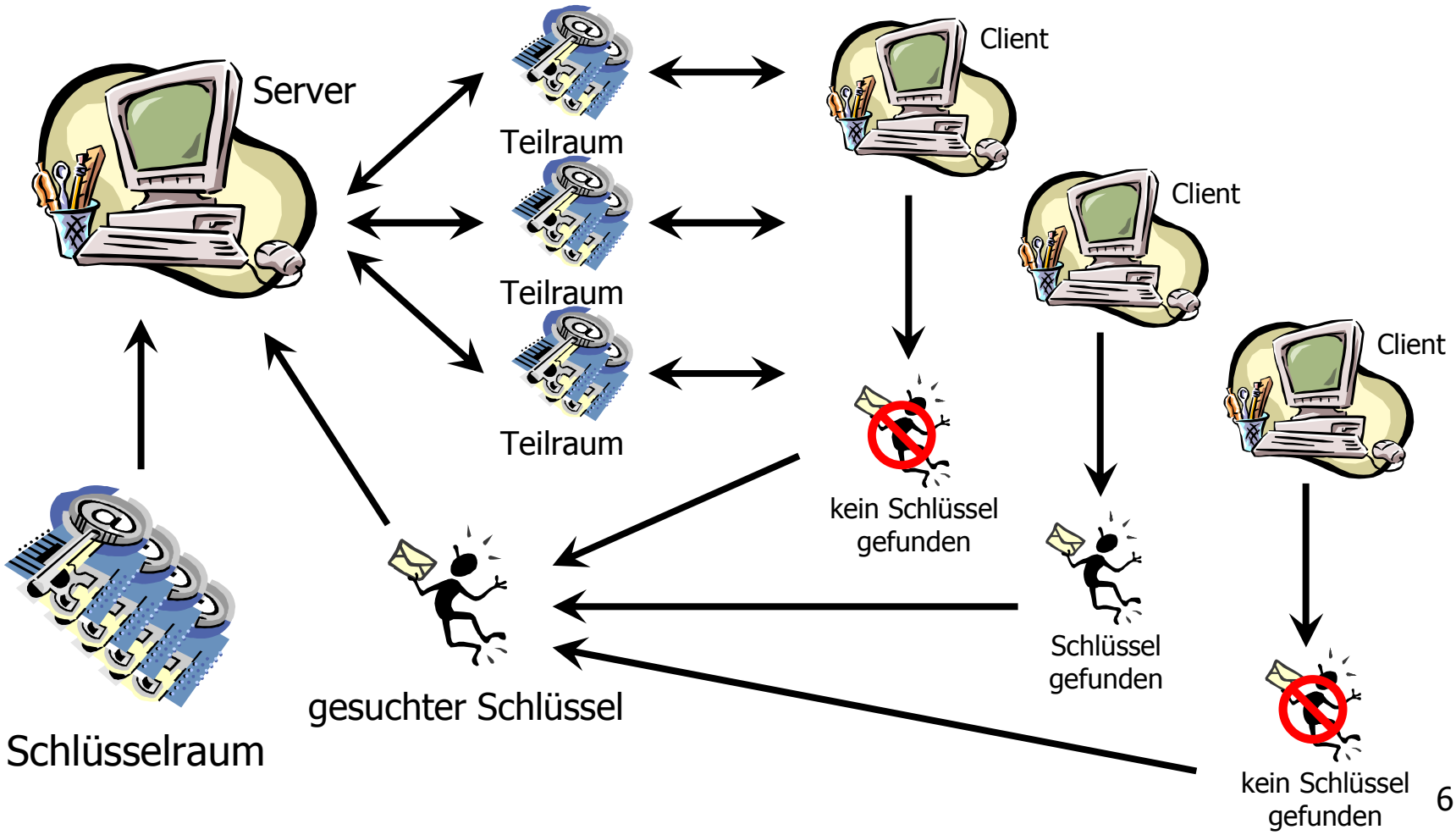


Einführung Traditioneller Crackvorgang

Schlüsselraum

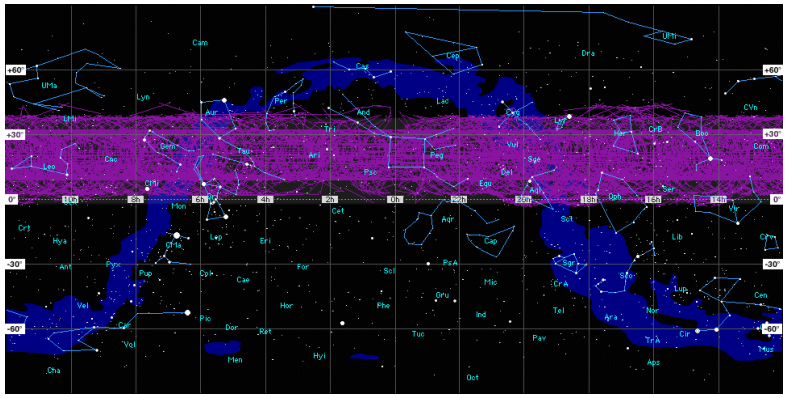
gesuchter Schlüssel

Einführung Server/Client-Crackvorgang



Einführung komplexe Aufgaben 1

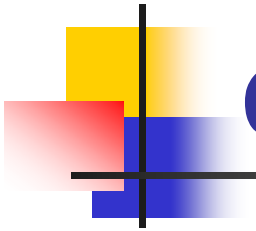
- Seti@Home
  - Suche nach Aliens
  - Clients durchsuchen aufgezeichnete Signale mittels Signaltransformation nach Signaturen



- RC5-64 & OGR24+
  - laufende Projekte bei distributed.net
  - dazu später mehr

Einführung komplexe Aufgaben 2

- MoneyBee
  - Ziel: Börsenkurse voraus zu berechnen
- FightAids@Home
  - Ziel: Aids zu bekämpfen
- Mars Clickworkers
  - nur begrenzt Distributed Computing
  - Ziel: Marskrater zu katalogisieren
- DDoS
  - Detail im Seminar von J. Zehnder

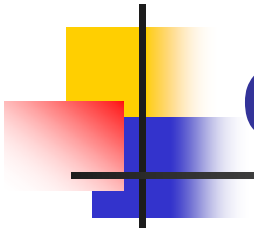


distributed.net Einleitung

- Organisation mit dem Ziel, die Entwicklung und die Förderung des verteilten Rechnens zur Lösung komplexer Aufgaben zu unterstützen.

- Nimmt an Wettbewerben teil
  - Rc5-64
  - OGR24+

- Bietet dazu Client-Software zum freien Download an

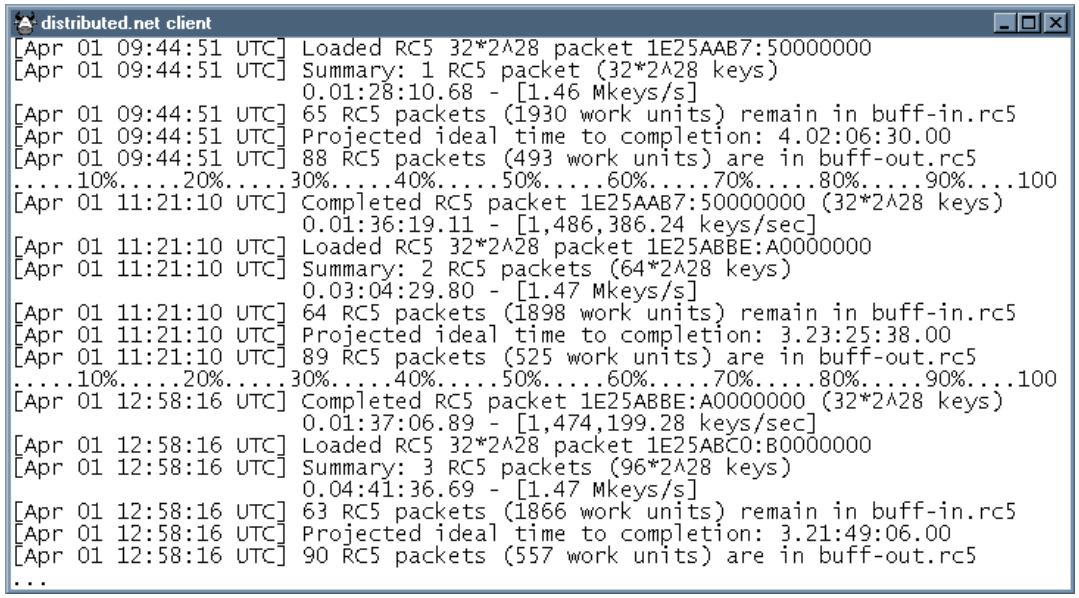


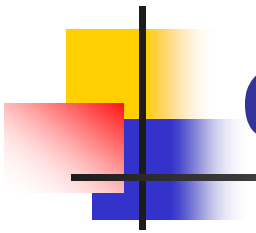
distributed.net Slogans

- Fans beschreiben die Seite und ihr Ziel so:
  - There is a place where Linux, Microsoft and Apple work happily together - distributed.net
  - Feel the Brute Force!
  - .... und wir knacken ihn doch
  - Faster than NSA!
  - distributed.net "Lets share the Power."
  - You've lost your key? - We'll find it.
  - Gotta' Crack 'em All!
  - ... because cpu time is a terrible thing to waste.

distributed.net RC5-64

- momentan wichtigstes Projekt bei distributed.net
- Versuch, einen 64bit-Schlüssel mit der BruteForce-Methode zu knacken (Known-plaintext-Attacke)

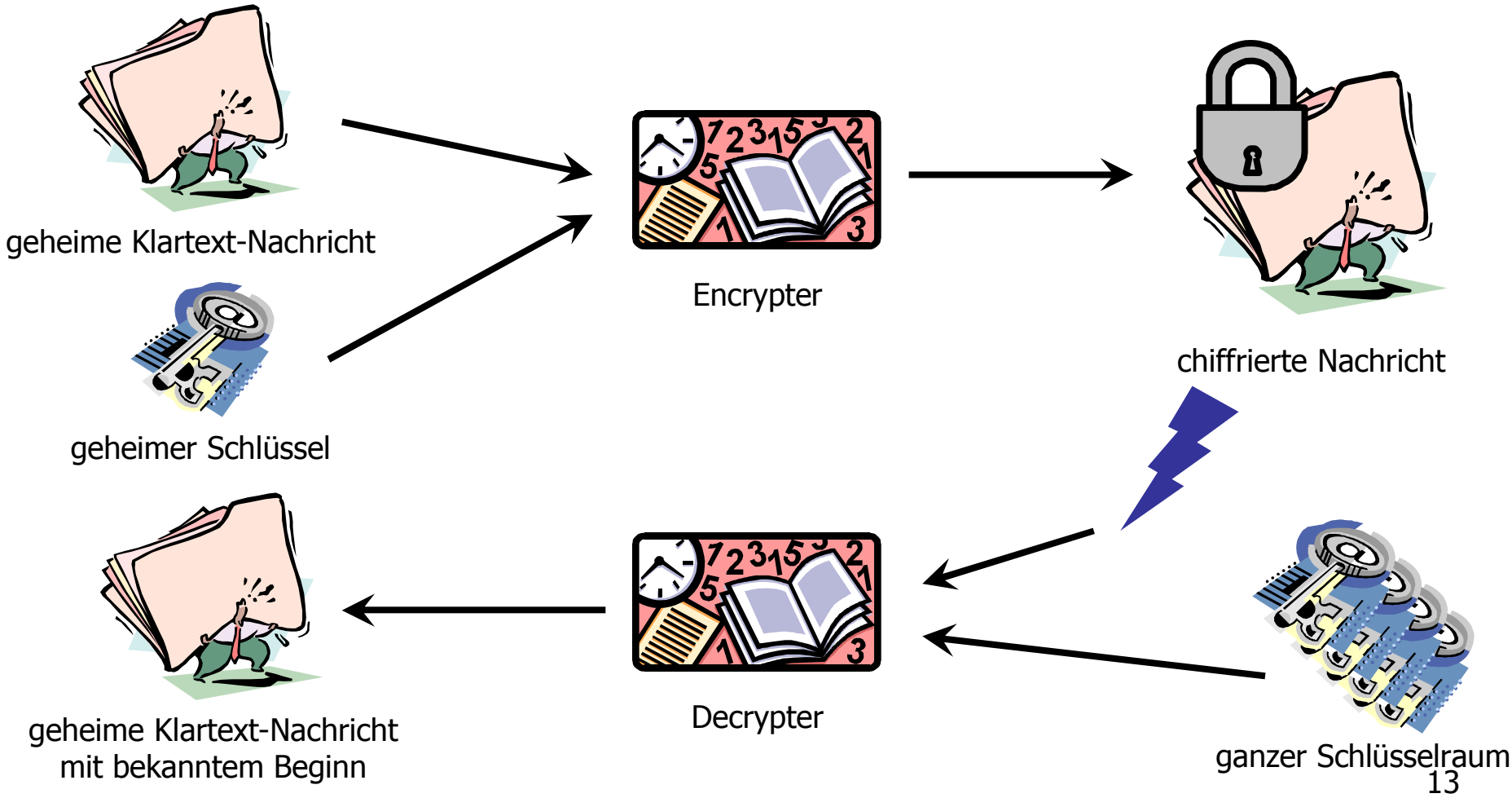


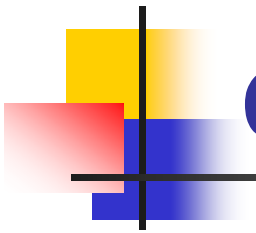


distributed.net RC5-64

- Falls distributed.net als erste Gruppe den Code knackt, stehen folgende Preise aus:
  - $1000 für den Finder
  - $1000 für das Team des Finders - diese gehen direkt an den Finder, wenn er nicht in einem Team ist
  - $6000 an eine gemeinnützige Gesellschaft, bestimmt durch die Teilnehmer
  - $2000 an distributed.net für den Aufbau des Netzwerks und das Bereitstellen der Clients

distributed.net RC5-BruteForce





distributed.net RC5-64

- Hochrechnung basierend auf der durchschnittlichen Einzelleistung am 25.03.01:

Schlüssel	56bit	64bit	128bit	512bit
Anzahl Bit	56	64	128	512
Anzahl Möglichkeiten	7.20576E+16	1.84467E+19	3.40282E+38	1.3408E+154
Dauer für Einzelrechner in Jahren	538	137878	2.5E+24	1E+140
Dauer bei 34595 Clients in Jahren	5.7 Tage	4	7.35E+19	2.9E+135

distributed.net OGR24+

- Suche nach optimalen Golomb-Massstäben
- Definition: Golomb-Massstab
  - Satz von positiven Zahlen, kein Paar der Zahlen hat den gleichen Abstand.

Markierung 1	Markierung 2	Abstand
0	1	1
0	4	4
0	9	9
0	11	11
1	4	3
1	9	8
1	11	10
4	9	5
4	11	7
9	11	2

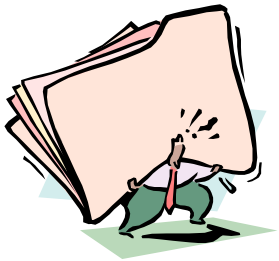
distributed.net Clients

- laufen als Hintergrundprozess
- niedrigste Priorität
- alternativ auch als ...
  - ... Serviceprozess
  - ... Screensaver

- erhältlich für viele Betriebssysteme:

Acorn RISCOS	AmigaOS	AIX	BeOS
OpenBSD	NetBSD	FreeBSD	BSD/OS
DEC UNIX/OSF1	PC-DOS/MS-DOS	HPUX	Linux
Mac OS X	Mac OS	Novell NetWare	NeXT/OS
IBM OS/2	IBM OS/390	QNX	SCO Unix
SGI IRIX	Sequent DYNIX	SINIX	Solaris/SunOS
DEC VMS	Windows 95/98/NT	Windows 3.x	

Demo Very-Simple-Java-Crack

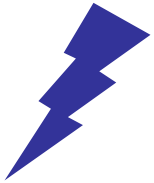


geheime Klartext-Zahl

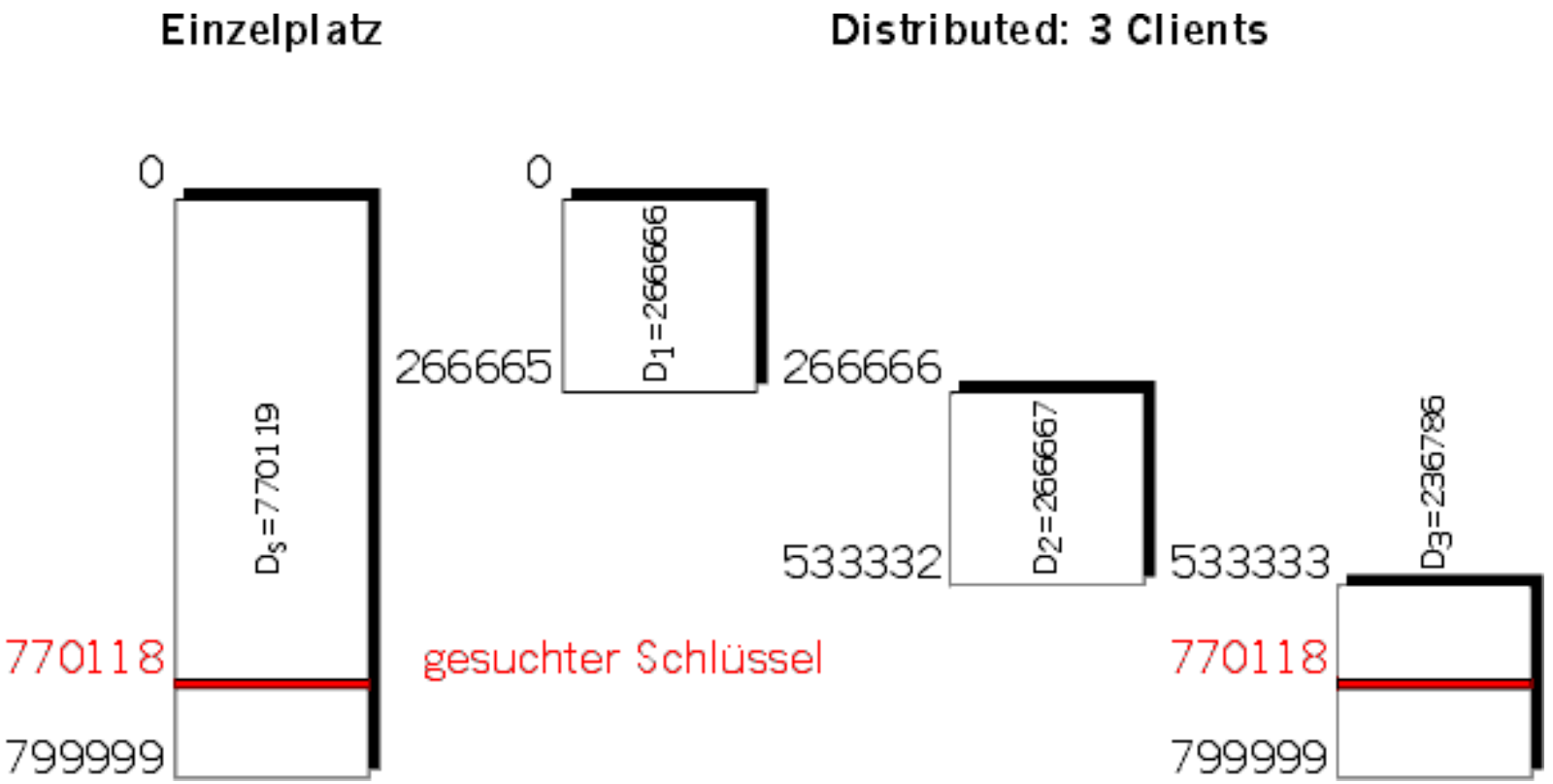
mathematische Transformation
(mit Delay implementiert)

chiffrierte Zahl

alle möglichen
Klartext-Zahlen



Demo Geschwindigkeitsgewinn



Demo DKBF Distributed-L0phtCrack

- DKBF nutzt Linux-Rechner als Cluster
- Pro Maschine ein L0phtCrack mit anderen Blöcken
- Eindrückliche Hochrechnung der Suchzeit

- 7C1S = 7 Clients & 1 Server

Bereich	Anz. Schlüssel	7C1S nach Dkbf in Stunden	Single-PC nach Dkbf in Stunden
A-Z	8'353'082'582	1	7
A-Z, 0-9	80'603'140'212	9	63
A-Z, 0-9, 33 Symbole	7'555'858'447'479	35 Tage	245 Tage

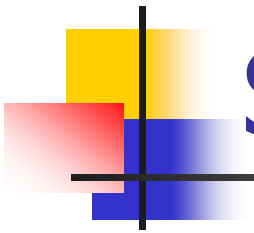
Bereich	Anz. Schlüssel	7C1S nach MiA in Stunden	Single-PC nach MiA in Stunden
A-Z	8'353'082'582	0	2
A-Z, 0-9	80'603'140'212	3	18
A-Z, 0-9, 33 Symbole	7'555'858'447'479	18 Tage	125 Tage

Zusammenfassung

- Sehr einfach, Aufgaben zu verteilen
- Cracking-Resultate teilweise sehr beeindruckend

Schlüssel	56bit	RC5-64	NT-Passwort
Dauer bei 34595 Clients	5.7 Tage	4 Jahre	
Dauer bei 7 Clients			max. 18 Tage

- Folgerung
  - Passwörter sollten mindestens RC5-64 Crackaufwand brauchen
- Nachteil
  - Niemand kann es sich noch merken



Sie werden Ihr Leben ändern!

- sofort Passwörter ändern
- nur noch Sonderzeichen verwenden
- wöchentlicher Wechsel der Passwörter
- Paranoia

oder

- täglicher Besuch auf distributed.net
- 7-fach-Linux-Cluster zulegen
- eigene Distributed-Software schreiben