

Diplomprüfung Praktische Informatik
Verteilte Systeme
Kurs 1678 - WS 1999/2000

Datum: 13.03.2000, 09.00 Uhr
Dauer: 25 Minuten
Prüfer: Prof. Dr. Unger
Beisitzer: Herr Lukosch
Note: 1,0

Bei der Prüfung ging es hauptsächlich um 3 Themen:

I. Datenübertragung in Verteilten Systemen:

Wie kann man sich vor möglichen Übertragungsfehlern in Verteilten Systemen schützen?
Parity-Bit, Hamming-Code, CRC-Prüfsumme

Wie funktioniert das CRC-Verfahren?
Verfahren detailliert beschrieben (s. Kurstext)

Welche Fehler können festgestellt werden?
...
Burst-Fehler bis zur Länge k

Was ist mit Bündelfehlern $> k$?
können fast alle erkannt werden

Warum nur fast alle?
Wahl des Polynoms $C(x)$ hat hier den entscheidenden Einfluß.
Fehlerpolynom $F(x)$ hat überall einen Koeffizienten, wo 1 Bit umgesprungen ist. Das übertragene Polynom $N(x)$ ist ohne Rest durch $C(x)$ teilbar, wenn dies auch für $F(x)$ zutrifft. $C(x)$ muß also so gewählt werden, daß möglichst wenig Fehlerpolynome durch $C(x)$ teilbar sind.

II. Kryptografische Verfahren:

Wie schützt man Nachrichten vor unberechtigtem Zugriff?
durch Verschlüsselung

Welche Verfahren gibt es hierzu?

DES-Verfahren
RSA-Verfahren

Auf welchen Mechanismen beruhen die Verfahren?
DES: public key, **Sender/Empfänger** müssen den Schlüssel kennen
RSA: private key, asymmetrisch, **Sender/Empfänger** geben öffentliche Schlüssel bekannt

Wie funktioniert das DES-Verfahren?
Grobe Beschreibung **des Verfahrens** (s. Kurstext)

Wie funktioniert das RSA-Verfahren?

Verschlüsselung/Entschlüsselung ausführlich beschrieben

Was ist die Symmetrie-Eigenschaft beim RSA-Verfahren?

Ver-/Entschlüsselung können in der Reihenfolge umgekehrt werden

Was erreicht man damit?

Authentisierung des Senders

Geschützte Übertragung zwischen Sender und Empfänger

III. Remote Procedure Call

Was ist ein RPC?

Ausführung eines Unterprogramms auf einem entfernten Rechner

Wie funktioniert ein RPC?

Benutzer -> Prozeduraufruf (Client) -> Verpacken der Parameter (Client-Stub) -> Senden (Kern des Client) -> Empfangen (Kern des Servers) -> Auspacken der Parameter (Server-Stub) -> Ausführen des Unterprogramms (Server) und zurück

Welche Schwierigkeiten können sich bei der Parameterübergabe ergeben?

Problematische Behandlung von Referenz-Parametern

Schwierigkeiten bei dynamischen Datenstrukturen (Listen, Bäume, . . .)

Die Prüfung verlief in lockerer Atmosphäre. Herr Unger ist sehr nett. Er verlangt nichts auswendig gelerntes, sondern ergründet durch seine Fragen, ob die Zusammenhänge sitzen.

Ich habe mich zur Vorbereitung intensiv mit dem Kurstext auseinandergesetzt und habe nichts auswendig gelernt, sondern versucht, die Zusammenhänge zu verstehen. Die Fragen zu den 3 Themen gingen im Stoff teilweise ziemlich tief, vor allem haben mich die Fragen zu den mathematischen Details beim RSA-Verfahren überrascht. An manchen Stellen mußte ich zunächst passen, durch gezielte Fragen von Prof. Unger konnte ich dann doch die gewünschten Antworten "online" erarbeiten.

Als Prüfer ist Herr Unger aus meiner Erfahrung uneingeschränkt zu empfehlen.

Viel Erfolg für Eure Prüfungen

Gerhard Dittmaier