Institutionen för Data- och Systemvetenskap

STOCKHOLMS UNIVERSITET

KUNGLIGA TEKNISKA HÖGSKOLAN

*:96 (SU) and 2I1263 (KTH) Internet Application Protocols and Standards

Exam 2004-12-04-solved.doc

The following documents are allowed during the exam:

1. Documents in Compendium 1, printed on colored paper.
2. Documents in Compendium 2, printed on colored paper.
3. Documents in Compendium 3, printed on colored paper.
4. Documents in Compendium 7, printed on colored paper.
5. Documents in Compendium 9, printed on colored paper.
6. Ordinary language dictionaries between English and Swedish.

Note 1: Compendium 0, 4, 5, 6 and 8 are not allowed during the exam.

Compendium 1-3, 7 and 9, printed on coloured paper, are allowed. Ordinary English-Swedish and Swedish-English dictionaries are also allowed. The exam supervisor will check that you do not have copies of the disallowed compendiums. Bringing such compendiums on colored paper is cheating and can result in suspension of your rights to study.

Note 2: Underscoring and short handwritten notes in the yellow documents are allowed.

Note 3: A few copies of the allowed compendiums will be available for loan during the exam for students who have not bought the compendiums.

Important warning

It is not acceptable to answer an exam question by just a verbatim quote from the allowed documents above. You must show that you understand the question and your answer by using your own words.

Jacob Palme will be available by phone 08-664 77 48, if you have need clarification of any question in the exam.

Continued on the next page

No.	Question in English	Question in Swedish	Max points
1	Dates can be written in a number of formats, as shown by these examples, all pertaining to the same date: 24 December 2004 24 Dec 2004 24 Dec 04 24-Dec-04 12/24/04 12/24/2004 Dec 24, 2004 December 24, 2004 Write an ABNF specification which covers all these formats (and more, if you know of more formats). The specification need not handle dates in other languages than English.	Datum kan skrivas i många olika format, som framgår av dessa exempel, som alla hänvisar till samma datum: 24 December 2004 24 Dec 2004 24 Dec 04 24-Dec-04 12/24/04 12/24/2004 Dec 24, 2004 December 24, 2004 Skriv en specifikation i ABNF som täcker syntaxen för alla dessa format (och fler, om du kan komma på något mer format). Specifikationen behöver inte klara av datum på andra språk än engelska.	6
2	What is the advantage with use of public key encryption as compared to secret key encryption? How is this advantage used for identification?	Vad är fördelarna att använda öppen-nyckel-kryptering jämfört med hemlig-nyckel-kryptering? Hur används denna fördel vid identifiering?	6

Answer:

day = 1*2D

month = "Jan" / "Feb" / ... / "Dec" / "January" / "February"/ ... / "December"

year = 2*D / 4*D

separator = "/" / "-" / " " / ","

date = day sep month sep year / month sep day sep year / year sep month sep day

No.	Question in English	Question in Swedish	Max points

Answer:

The advantage with public key encryption, as compared to secret key encryption, is that the public key can be transported without keeping it secret, and that anyone can get the public key without risking your security. However, the transport must still be protected from tampering while the key is being sent.

For identification, the agent requesting identification sends a random string and gets it back encrypted with the secret key of the agent to be identified. The agent requesting identification then decrypts this with the public key, and checks if the result is the same random string that was originally sent.

3	Which methods are available in HTTP for ensuring that a cache does not provide stale information?	Vilka metoder finns i HTTP för att hindra att en cache levererar föråldrad information?	6

Answer:

Command	Use	Means
Cache-Control	Request	See below
Cache-Control: no-cache=field-name	Request	Do not use cached copy
Cache-Control: no-store	Request, Response	Do not store on discs for security reasons (discs might be backed-up)
Cache-Control: max-age=	Request	Client can accept a response which is not older than this time, similar to Expires
Cache-Control: min-fresh=	Request	Client wants response which is valid a certain minimum time
Cache-Control: max-stale=	Request	Client can accept stale data
Cache-Control: only-if-cached	Request	Return only cached data, not data from the original server
Cache-Control: public=field-name	Response	Can be cached and later used for someone else
Cache-Control:	Response	Can only be cached for use by this

Command	Use	Means
private=field-name		particular user
Cache-Control: no-transform	Response	Do not cache in media-converted format
Cache-Control: must-revalidate	Response	Always revalidate stale cached data
Cache-Control: proxy-revalidate	Response	Same as must-revalidate, but not for user agent caches
Expires: Absolute date	Response	Refresh cache if cached copy is older than this date
Expires: 0	Response	Same as "Expires immediately".
Pragma: No-Cache	Request	Old alternative to Cache-Control
Guessing expiration date based on age		

4 Why is there a need for a registry organisation like IANA and ICANN? Give at least two examples of parameters registered by these organisations.

Varför behövs en registrerings-myndighet, som IANA och ICANN? Ge minst två exempel på parametrar som dessa myndigheter registrerar. 6

Answer:

Certain identifiers need to have a unique name, which is the same everywhere. This is needed for example for domain names, if two different computers had the same domain name, A client establishing a connection would not know which computer to connect to. In the same way, port numbers need to be standardized so that for example a HTTP client gets connected to an HTTP server and not to an SMTP server, which does not speak HTTP. And names of MIME types need to be standardized so that sending and receiving computer can agree on the format of the content, and not for example try to open a Microsoft Word file with a program for opening JPEG files.