VerteilteWebInf Hausaufgabe 10

Gruppe 6

January 5, 2015

Aufgabe 1

Die Benchmarks wurden auf einem Macbook Pro, 3 GHz Intel Core i7, 8GB Ram mit Java 7 (64 Bit) durchgeführt. Alle Zeitangaben sind in Millisekunden (ms). Gestartet wird jeder Benchmark mit einer leeren Datenbank. Beim Einfügen wird jeder Datensatz einzeln eingefügt (kein Batch-Opertion). Nachdem alle Datensätze eingefügt worden sind wird einzeln nach jedem Element gesucht (query). Anschließend wurde jedes Element einzeln wieder aus der Datenbank gelöscht.

1 Telefonbucheintrag

Operation	**HashMap**	**MongoDB**	**mdbm**
Insert insgesamt	0	12	-
Insert / Datensatz	0	12	-
Query insgesamt	0	3	-
Query / Datensatz	0	3	-
Delete insegesamt	0	2	-
Delete / Datensatz	0	2	-

10 Telefonbucheintrag

Operation	**HashMap**	**MongoDB**	**mdbm**
Insert insgesamt	0	16	-
Insert / Datensatz	0	1,6	-
Query insgesamt	0	6	-
Query / Datensatz	0	0,6	-
Delete insegesamt	0	6	-
Delete / Datensatz	0	0,6	-

100 Telefonbucheintrag

Operation	HashMap	MongoDB	mdbm
Insert insgesamt	0	82	-
Insert / Datensatz	0	0,8	-
Query insgesamt	0	52	-
Query / Datensatz	0	0,5	-
Delete insegesamt	0	81	-
Delete / Datensatz	0	0,8	-

1.000 Telefonbucheintrag

Operation	HashMap	MongoDB	mdbm
Insert insgesamt	1	417	-
Insert / Datensatz	0	0,4	-
Query insgesamt	0	235	-
Query / Datensatz	0	0,2	-
Delete insegesamt	0	354	-
Delete / Datensatz	0	0,3	-

100.000 Telefonbucheintrag

Operation	HashMap	MongoDB	mdbm
Insert insgesamt	16	13.202	-
Insert / Datensatz	0	0,1	-
Query insgesamt	12	10.724	-
Query / Datensatz	0	0,1	-
Delete insegesamt	15	14.670	-
Delete / Datensatz	0	0,1	-

1.000.000 Telefonbucheintrag

Operation	HashMap	MongoDB	mdbm
Insert insgesamt	253	115.327	-
Insert / Datensatz	0	0,1	-
Query insgesamt	62	105.306	-
Query / Datensatz	0	0,1	-
Delete insegesamt	73	159.931	-
Delete / Datensatz	0	0,1	-

5.000.000 Telefonbucheintrag

Operation	HashMap	MongoDB	mdbm
Insert insgesamt	2544	651.543	-
Insert / Datensatz	0	0,1	-
Query insgesamt	816	548.228	-
Query / Datensatz	0	0,1	-
Delete insegesamt	73	841.528	-
Delete / Datensatz	0	0,1	-

Aufgabe 2

b)
gegeben: verschlüsselte Nachricht $C = 13$, öffentlicher Exponent $e = 3$, $n = p \cdot q = 15$

Der Klartext M kann über $C^d \mod n$ berechnet werden, wobei d der private Exponent des Empfängers ist.
Berechne d: Es muss gelten, dass $e \cdot d \equiv 1 \mod \Phi(n)$ mit $\Phi(n) = (p-1)(q-1)$.
Wir benötigen also Primzahlen p und q, sodass $p \cdot q = n = 15$: $p = 3$, $q = 5$.
Also gilt $\Phi(n) = 4 \cdot 2 = 8$.
Es muss also gelten: $3 \cdot d \equiv 1 \mod 8$, also wähle $d = 3$.
Klartext $M = C^d \mod n = 13^3 \mod 15 = 7$. Der Klartext der Nachricht lautet also 7.