

Modular Exponentiation Algorithm

b = 429
 n = 734
 m = 253

$(n)_{16} = 2DE$

Computing $(429^{734}) \bmod 253 = 165$

<i>i</i>	<i>x</i>	<i>power</i>	<i>a_i</i>	new <i>X</i>		new <i>power</i>	
				Formula	Value	Formula	Value
					1	$429 \bmod 253 =$	176
0	1	176	0		1	$(176 * 176) \bmod 253 =$	110
1	1	110	1	$(1 * 110) \bmod 253 =$	110	$(110 * 110) \bmod 253 =$	209
2	110	209	1	$(110 * 209) \bmod 253 =$	220	$(209 * 209) \bmod 253 =$	165
3	220	165	1	$(220 * 165) \bmod 253 =$	121	$(165 * 165) \bmod 253 =$	154
4	121	154	1	$(121 * 154) \bmod 253 =$	165	$(154 * 154) \bmod 253 =$	187
5	165	187	0		165	$(187 * 187) \bmod 253 =$	55
6	165	55	1	$(165 * 55) \bmod 253 =$	220	$(55 * 55) \bmod 253 =$	242
7	220	242	1	$(220 * 242) \bmod 253 =$	110	$(242 * 242) \bmod 253 =$	121
8	110	121	0		110	$(121 * 121) \bmod 253 =$	220
9	110	220	1	$(110 * 220) \bmod 253 =$	165		