Построить подпись RSA для сообщения m при следующих параметрах пользователя:

а. $P = 5$, $Q = 11$, $c = 27$, $m = 7$,

б. $P = 5$, $Q = 13$, $c = 29$, $m = 10$,

в. $P = 7$, $Q = 11$, $c = 43$, $m = 5$,

г. $P = 7$, $Q = 13$, $c = 29$, $m = 15$,

д. $P = 3$, $Q = 11$, $c = 7$, $m = 24$.

Для указаннных открытых ключей пользователя RSA проверить подлинность подписанных сообщений:

а. $N = 55$, $d = 3$: $\langle 7, 28\rangle$, $\langle 22, 15\rangle$, $\langle 16, 36\rangle$,

б. $N = 65$, $d = 5$: $\langle 6, 42\rangle$, $\langle 10, 30\rangle$, $\langle 6, 41\rangle$,

в. $N = 77$, $d = 7$: $\langle 13, 41\rangle$, $\langle 11, 28\rangle$, $\langle 5, 26\rangle$,

г. $N = 91$, $d = 5$: $\langle 15, 71\rangle$, $\langle 11, 46\rangle$, $\langle 16, 74\rangle$,

д. $N = 33$, $d = 3$: $\langle 10, 14\rangle$, $\langle 24, 18\rangle$, $\langle 17, 8\rangle$.

Абоненты некоторой сети применяют подпись Эль-Гамаля с общими параметрами $p = 23$, $g = 5$. Для указанных секретных параметров абонентов найти открытый ключ (y) и построить подпись для сообщения m:

а. $x = 11$, $k = 3$, $m = h = 15$,

б. $x = 10$, $k = 15$, $m = h = 5$,

в. $x = 3$, $k = 13$, $m = h = 8$,

г. $x = 18$, $k = 7$, $m = h = 5$,

д. $x = 9$, $k = 19$, $m = h = 15$.

Для указаннных открытых ключей (y) пользователей системы Эль-Гамаля с общими параметрами $p = 23$, $g = 5$ проверить подлинность подписанных сообщений:

а. $y = 22$: $\langle 15; 20, 3\rangle$, $\langle 15; 10, 5\rangle$, $\langle 15; 19, 3\rangle$,

б. $y = 9$: $\langle 5; 19, 17\rangle$, $\langle 7; 17, 8\rangle$, $\langle 6; 17, 8\rangle$,

в. $y = 10$: $\langle 3; 17, 12\rangle$, $\langle 2; 17, 12\rangle$, $\langle 8; 21, 11\rangle$,

г. $y = 6$: $\langle 5; 17, 1\rangle$, $\langle 5; 11, 3\rangle$, $\langle 5; 17, 10\rangle$,

д. $y = 11$: $\langle 15; 7, 1\rangle$, $\langle 10; 15, 3\rangle$, $\langle 15; 7, 16\rangle$.

Сообщество пользователей ГОСТа Р34.10-94 имеют общие параметы $q = 11$, $p = 67$, $a = 25$. Вычислить открытый ключ (y) и построить подпись для сообщения m при следующих секретных параметрах:

а. $x = 3$, $h = m = 10$, $k = 1$,

б. $x = 8$, $h = m = 1$, $k = 3$,

в. $x = 5$, $h = m = 5$, $k = 9$,

г. $x = 2$, $h = m = 6$, $k = 7$,

д. $x = 9$, $h = m = 7$, $k = 5$.

Для указаннных открытых ключей (y) пользователей ГОСТа Р34.10-94 с общими параметрами $q = 11$, $p = 67$, $a = 25$ проверить подлинность подписанных сообщений:

а. $y = 14$: $\langle 10; 4, 5\rangle$, $\langle 10; 7, 5\rangle$, $\langle 10; 3, 8\rangle$,

б. $y = 24$: $\langle 1; 3, 5\rangle$, $\langle 1; 4, 3\rangle$, $\langle 1; 4, 5\rangle$,

в. $y = 40$: $\langle 7; 7, 4\rangle$, $\langle 7; 9, 2\rangle$, $\langle 5; 9, 2\rangle$,

г. $y = 22$: $\langle 6; 9, 5\rangle$, $\langle 8; 8, 3\rangle$, $\langle 7; 4, 1\rangle$,

д. $y = 64$: $\langle 10; 7, 3\rangle$, $\langle 7; 7, 10\rangle$, $\langle 8; 7, 5\rangle$.