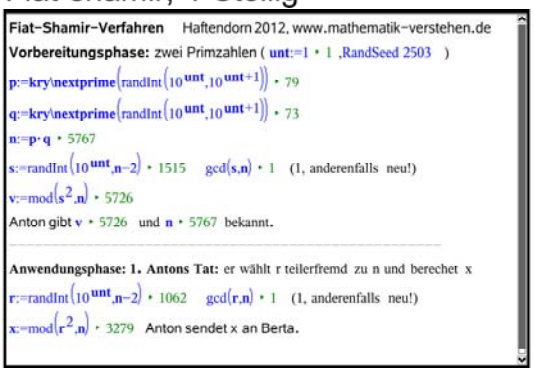
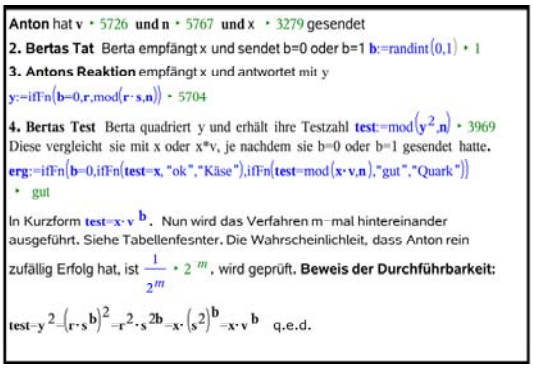
Fiat-shamir, 4-Stellig



1.1

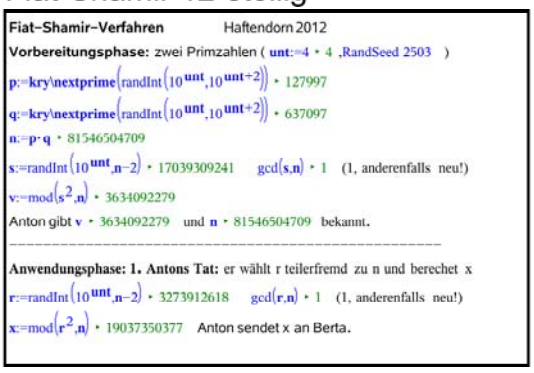


1.2

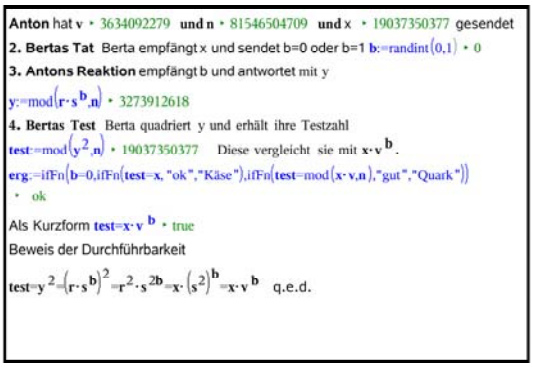
	A bit	B lir	C lix	D liy	E litest	F litestre	G	H
•	=seq(rand	=seq(rand	=mod(lir^2	=mod(lir*s	=mod(liy^2,	=mod(lix*		
1	1	5400	2048	5400	2048	2048		
2	1	2397	1677	2397	1677	1677		
3	0	4952	1020	4952	1020	1020		
4	1	977	2974	3803	4940	4940		
5	0	5542	4489	5542	4489	4489		
6	1	541	4331	701	1206	1206		
7	0	2047	3367	4326	361	361		
8	0	5471	1111	1386	585	585		
9	1	1509	4883	2403	1642	1642		
10	0	1823	1537	5219	420	420		
11	1	3411	2882	433	2945	2945		
12	1	1490	5572	2453	2228	2228		
13	0	3477	1897	3477	1897	1897		
14	0	5064	4014	1850	2669	2669		
A1	=1							

1.3

Fiat-Shamir 12-stellig

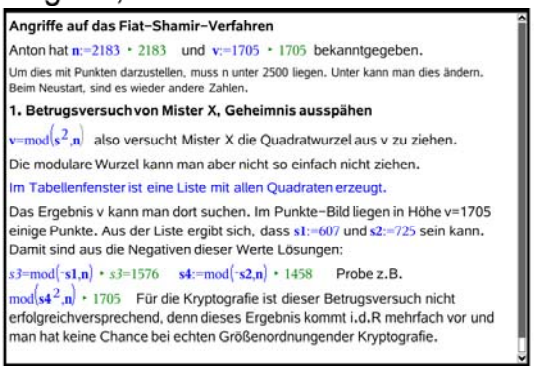


2.1



2.2

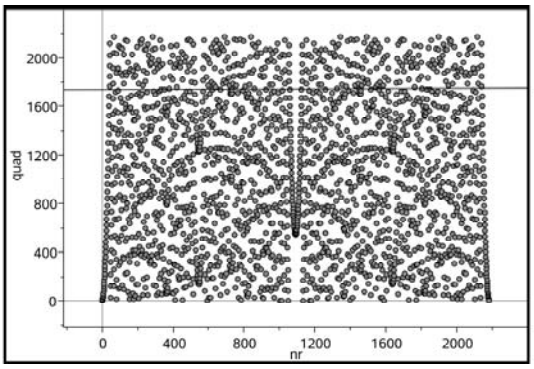
Angriffe, direkt



3.1

	A nr	B quad	C	D	E	F	G	H
•	=seq(i,i,1,	=mod(nr^2,	=iffn(quad					
1	1	1	0					
2	2	4	0					
3	3	9	0					
4	4	16	0					
5	5	25	0					
6	6	36	0					
7	7	49	0					
8	8	64	0					
9	9	81	0					
10	10	100	0					
11	11	121	0					
12	12	144	0					
13	13	169	0					
14	14	196	0					
E64								

3.2

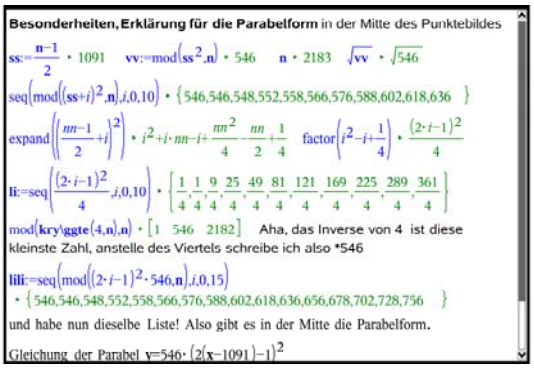


3.3

	A bit	B lir	C lirq	D lisx_	E litest	F litestre	G	H
•	=seq(rand	=seq(rand	=mod(lir^2,'i	=mod(lirq*	=lirq	=mod(lisx_		
1	0	1219	358	358	358	358		
2	0	822	728	921	728	728		
3	0	1964	1701	2047	1701	1701		
4	0	599	2093	192	2093	2093		
5	1	932	248	248	248	248		
6	0	1980	271	271	271	271		
7	0	1494	2106	2106	2106	2106		
8	0	1010	1936	818	1936	1936		
9	0	324	182	182	182	182		
10	1	2066	736	1195	736	736		
11	1	1814	323	1785	323	323		
12	0	1141	400	400	400	400		
13	1	221	855	359	855	855		
14	0	1731	1554	1924	1554	1554		

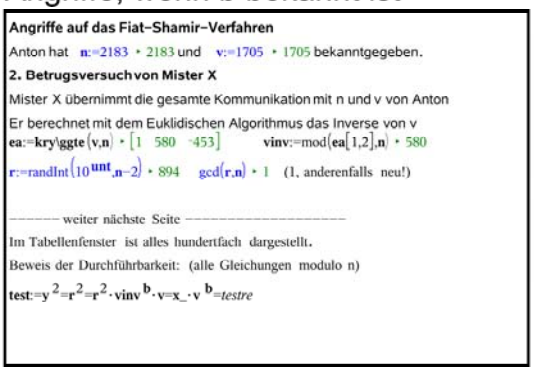
E6 =271

3.4

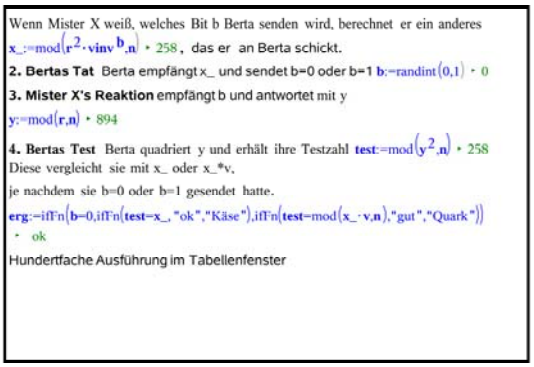


3.5

Angriffe, wenn b bekannt ist



4.1



4.2

	A bit	D lir	C lix_	D liy	E litest	F litestre	G	H
•	=seq(rand	=seq(mod	=mod('li	=lir	=mod(liy^2	=mod(lix_		
1	0	1160	872	1160	872	872		
2	0	1102	638	1102	656	656		
3	1	1014	1740	1014	3	3		
4	1	2084	48	2084	1069	1069		
5	1	452	1285	452	1285	1285		
6	1	771	665	771	665	665		
7	1	1313	1582	1313	1582	1582		
8	0	1895	749	1895	2173	2173		
9	1	2018	1029	2018	1029	1029		
10	0	1950	28	1950	1897	1897		
11	1	272	1672	272	1945	1945		
12	0	878	285	878	285	285		
13	0	1904	1157	1904	1436	1436		
14	0	419	1528	419	921	921		

G

4.3