Asymmetric attacks: assessment

CATALDO BASILE

< CATALDO.BASILE@ POLITO.IT >

POLITECNICO DI TORINO

Preliminary stats

Please fill in this form as I use it for statistical purposes

- https://docs.google.com/forms/d/e/1FAIpQLSfbhSoo-lB-nK-1rckXiea2Okhf9TeDKa2Nj0AXtdwa4yB6aQ/viewform

Understand numbers #1

x1 =(
109122243636469707550711018195661170687409619107532053553306250129905193715844004112816834344622610785356382664692203912843067357302351546903609936807703727741692915627850414111929732731908052202645655422306346673568740831090084301971250700436296324714879489767394365348533252987621946447152355790698729847829,
3,739715821722217209754802901806577828566307314125013968970390882868237907521224402410669353459421120428974589010870256517729332511565241419536557957535787332029924065638394190648914604442214359026199024005620128556582833392556817010884093826769509304752658382952589 04)

- form
  - https://docs.google.com/forms/d/e/1FAIpQLSfjzWiqGlHpdKFmWmIxyurqxtc00F9FMp8kSrfHs3EpjI6rvw/viewform?usp=dialog

Understand numbers #2

C1 =
125363708807577101691189344679176506572
649828408511764802565240477127331639726
928767037931192035651617508152535805480
780938975688036592214381822686438816700
984251795742219051754443750511906635212
337268172914754823669225677323029362087
248170814798222127100240931034778518466
301289309026296726395563814389944466

N1 =
137887122568531770052906670751836781371
188547817912681827699459229601457856092
485235031470842764497111130242984479898
854823665959881623318103414349936603413
367355821161134641346923895414637259410
038068321634553398760005906725246088771
693891835733407419032210967175403657580
025716770208117204192371608966464447

p1 = (C1, 5, N1)

- form
  - https://docs.google.com/forms/d/e/1FAIpQLScEI2DGtmmBxoUCctsOEJnMO9J5jnDJsjrwWVr9jWNV-Q_V-w/viewform?usp=dialog

Understand numbers #3

(20619672002276824788924668
00664375981780200323053931
19870540720920425094195833
61298447954874234536130293
26452196390948676768692154
17348824384613993692025679
42513149981123162909089349
13863837212956458092446009
35874119405837136909758154
1094913, 65537)

- form
  - https://docs.google.com/forms/d/e/1FAIpQLSe_i1JqSCy_LaS3l59NR_JmLx5MSKkH6xjJlDxlJxD5EURGFw/viewform?usp=dialog

Strange RSA key generation

k0 = (65537,
15939612455866939079935976033180753684002925572002216890105223178260228002670318464859333274408486343831876984019368596197373095375299589845685218641557668528225361765545757838424864421384161133908890208471463526982048721755139638775901833121435695768676630452584156922991771117870642637722884525014230011611311810110415005748878808871881794230480334327081278239624270522408545402555004478337020662813734346485505519651890298132507226893420184846948591535594782823344867527472639774245410356348267893110619017344739561357894390726624852189170422685337970011953697064494544145036366470071491859450373255258072246348789)
k1 = (65537,
12506468603717061066741650068819664666546013916767845176695484215565918989154540123473153809163957285304753346873348420722258867253664588091724042089605119475976539293654927168430221190561080069853252345385934867955627892540549252074525873229577015702593473590176687071222280113815574729145042891414814498723660059120861450789566454998447391212337762406803917039520479065026101399083823639689497118601731170016207190090667686859063822668960788144186179420088118680455637872438198628518194947919329905421211015441192687589649666486897145140629676007899300794561464514688221098198032041078816985702649024295116040925153)

- form
  - https://docs.google.com/forms/d/e/1FAIpQLSc-L4iXUq0oUNgWA3s1eT3-JRqVEZBV8DAYWbO4SM8skH5DaQ/viewform?usp=dialog