

Prime candidate:
NTT Award



Can we factor RSA?

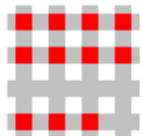
@k4403

@MarriageTheorem

@onix105

@factoring_bot

返信



k4403

4403



この話はSCIS2010ナイトセッション（2010年1月21日）の後日談です.

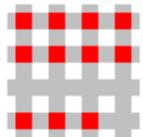


今日のおはなし



我々の研究チームでは768ビットの素因数分解^{*1}に負けないインパクトを世界に与えるべくRSAに対する画期的な攻撃を試みた.

今回は素因数分解ボット「ふあくたん^{*2}」を用いたRSAに対する新しい素因数分解攻撃法を紹介する.

[返信](#)

k4403

4403

*1 NTT et al. <http://bit.ly/aVN3aX>

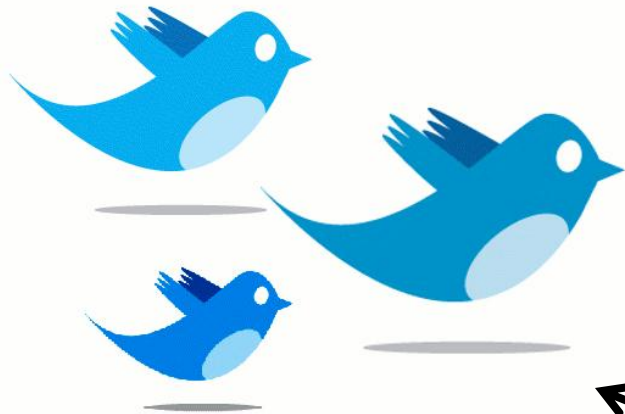
*2 @factoring_bot, 愛称「ふあくたん」

ふあくたん？

factoring_bot??

アルゴリズムとモデル図

Twitter



1. つぶやきの取得

4. RTでつぶやく



アルゴリズム

1. つぶやきの取得
2. つぶやきから素因数分解対象の数字を探す
3. 数字を既知素数表の小さい素数で順番に割っていく
4. 結果をRTでつぶやく

2-3. 素因数分解をするなど

注※開発速度を最優先としてPHPで実装した

factoring_botとfactrbotの関係

類似botにご注意ください

factoring_botとfactrbotの関係につきまして、
フォロワーの方からご意見が寄せられており
ますが、両botは、それぞれ**設計思想と技術的背景**を異にする別々のプログラマが設置した別々のbotであり、姉妹bot等の関係は一切ありません。



そんな素因数分解で大丈夫か？



大丈夫だ，問題ない．

神は言っている．素因数分解に時間がかかりすぎると．



@factrbot
素因数分解bot

@kmaro 100000000140000000049の素因数分解に時間がかかりすぎるため素因数分解を中止しました。別の数値を入力してください><[10/1 18:29:12]

6:29 PM 10月 1日 yakibot2から ☆お気に入り 🔄リツイート ↩返信



@factrbot

素因数分解bot

@kmaro 同じことは言わないよ > < [10/1
19:2:54]

7:02 PM 10月 1日 yakibot2から ☆お気に入り ↺リツイート ↩返信



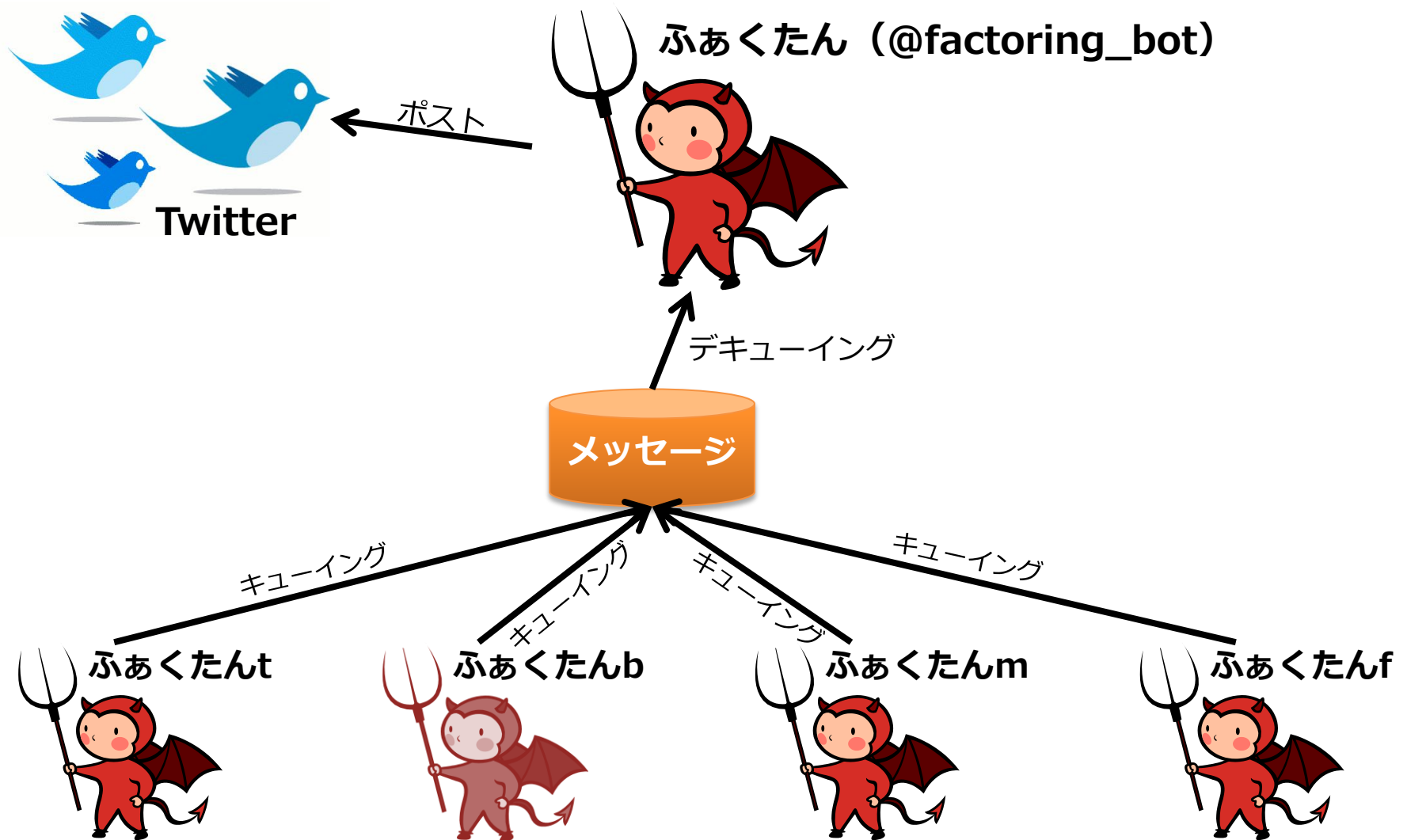
そんな素因数分解で大丈夫か？



一番良い素因数分解を頼む.

引用 ; <http://bit.ly/d2mKYY>

メッセージキューイング方式



Do you know them?



Rivest, out!



19470506=2*11*885023 RT

@[MarriageTheorem](#):

@[factoring_bot](#) 19470506

1:05 AM Jan 27th via [API](#)



factoring_bot

素因数分解ボット「ふあくたん」



返信

Ron Rivest
May 6, 1947
19470506

Shamir, out!



調べたらシャミアは偶数日生まれ。
シャミア乙。

12:05 AM Jan 27th via [Echofon](#)



onix105

Ryoichi Teramura



返信

Adi Shamir
July 6, 1952
19520706

Adleman, out!



19451231=19*71*14419 RT

@[MarriageTheorem](#):

@[factoring_bot](#) 19451231



返信

1:10 AM Jan 27th via [API](#)



[factoring_bot](#)

素因数分解ボット「ふあくたん」

Leo Adleman
December 31, 1945
19451231

ここまでのまとめ

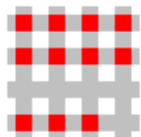


R 19470506 (even) = $2 * 11 * 885023$

S 19520706 (even) = $2 * 3 * 199 * 16349$

A 19451231 (odd) = $19 * 71 * 14419$

RSA is factored!

[返信](#)

k4403

4403

RSA乙



1月27日深夜、RSAの誕生日が全て合成数であることが@[factoring_bot](#)の調べでわかりました（ただし誕生日のソースは日本語版Wikipedia）。

返信

[1:12 AM Jan 27th](#) via web

No
絵心

MarriageTheorem

MarriageTheorem

これこそまさに

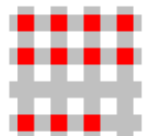


birthday

誕生日攻撃

attack

 返信



k4403

4403

ところで

時を同じくして

新しい学説が
浮上しました

新約セキュリティ研究者



19850113 is prime! RT @onix105:
@factoring_bot 19850113

返信

11:00 PM Jan 26th via API



factoring_bot

素因数分解ボット「ふあくたん」

誕生日素数は セキュリティ研究者の 必須要件か？



誕生日素数はセキュリティの人間としての必要条件に違いない。偶数日生まれ乙。 RT @[factoring_bot](#):
19850113 is prime!

返信

11:09 PM Jan 26th via [Echofon](#)



onix105

Ryoichi Teramura

@onix105提唱の
「新約セキュリティ研究者」
は正しいのか？

かくして

Twitter上の
セキュリティ研究者が
自分の誕生日をさらしはじめる
(個人情報漏洩事件)

結果！！

新約セキュリティ研究者

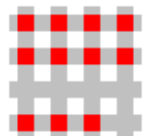


@onix105 19850113 is prime!

@k4403 19800731 is prime!

@minakoneko 19780907 is prime!

← 返信



k4403

4403

誕生日が素数の確率は？



1900年から2010年までの日付のうち8桁表現が素数なのは2484日ありましたので、**確率は約1/16**であることがわかりました。 RT @tohki: 誰か1900年以降に生まれた人の誕生日が素数になる確率とか計算しないかなあ

返信

7:53 PM Jan 27th via Saezuri



zusanzusan

杜撰な研究者

Appendix

NTTPR 人気あります



[ログイン](#) [ユーザー登録\(無](#)

つなぐ。
それは、
ECO

【大手町OLの豆知識-トークの日①-】NTTは1986年に毎月19日を「トークの日」と決めました。当時のニュースリリース資料によると、社内外からいただいた「コミュニケーションを考え、人と人とのふれあいを大切にする日を設けてはどうか」とのご意見をふまえ創設したもののようです。

9:20 PM May 18th webから [B!](#)



NTTPR
NTT広報室



$1986=2*3*331$ @[NTTPR](#)

返信

1:25 PM May 19th [factoring_bot](#)から [NTTPR宛](#)



factoring_bot

素因数分解ボット「ふあくたん」

つなく。
それは、
ECO 



申し訳ございませんが電話番号をお確か
めの上再度おかけ直してください。RT

@factoring_bot 1986=2*3*331

@NTTPR

2:27 AM May 19th webから 



NTTPR

NTT広報室

NHK_PR 面白いです

twitter

ログイン ユーザー登録

明日22日(土)は、13:00からBS1で「W杯
ジャパンプルーに託す夢」(<http://bit.ly/9oeM5u>)。なんと11時間の放送です。イ
レブンだから11時間？ 深夜0:00から「W杯
1986年メキシコ大会 準々決勝」。

<http://bit.ly/deBbNN>

2:00 AM May 21st HootSuiteから 



NHK_PR

NHK広報局



$1986 = 2 * 3 * 331$ @[NHK_PR](#)

← 返信

6:05 PM May 21st [factoring_bot](#)から [NHK_PR](#)宛



factoring_bot

素因数分解ボット「ふぁくたん」

> @factoring_bot サッカーですから、全部イレブンでやりましょうよ！
 $1986 = (11/11 + 11 + 11 + 11 * 11 + 11 / 11 + 11 * 11 + 11 * 11 + 11 / 11 + 11 * 11 * 11 + 11 / 11 + 11 * 11 + 11 / 11 + 11 * 11 + 11 + 11 + 11 / 11)$

2:27 AM May 21st HootSuiteから factoring_bot宛 



NHK_PR

NHK広報局

ちなみに

kddipr

は絡んできたか？



ついにやりました。(伊) RT
@[factoring_bot](#) 20100527 is
prime!

 返信

[10:19 AM May 27th](#) webから



kddipr
kddipr

ところで

つなぐ。
それは、
ECO



??

リーマンセンパイイ！！また天敵が現れましたよ！！ RT @factoring_bot
 $110 = 2 * 5 * 11$ RT @NTTPR: [報道発表]
[NTTファシリティーズ]3次元振動試験システム「DUAL FORCEの運用開始について
～「世界初」最大振動変位±110cmの振動

11:21 PM May 23rd webから



NTTPR

NTT広報室



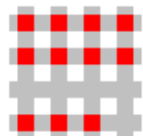
そこは

「カズマロセンパイイイ！！」

が正しいのではないだろうか.

NTT的な意味で.

 返信



k4403

4403