



刊行物登録番号
3-2-156

ぽけっと 3月

北区図書館情報

発行：令和5年3月
北区立中央図書館
〒114-0033
北区十条台1-2-5
TEL (5993) 1125
FAX (5993) 1044



情報セキュリティと素数～RSA暗号の話～



2023年も3月となりました。北区立図書館では、年始より新しい図書館システムが稼働し、利用者の皆様により良い図書館環境を提供できるよう努めております。

突然ですが、皆様は「3」と聞いて何を思い浮かべますか？

早起きは三文の徳、仏の顔も三度まで…など、人により様々かと思いますが、「3」は数学の用語で「素数」と呼ばれています。素数とは、2以上の数のうち1とその数自身以外で割り切ることができない数で、2、3、5、7、11…と無限に続きます。

普段の生活で素数を意識することは無いかもしれませんが、実は電子メールの送受信など情報セキュリティに素数が活用されています。

そこで、今月は「情報セキュリティ」と「素数」の関係について紹介します。

現代では、コンピューターで様々な情報がやり取りされていますが、世の中には他人の情報を不正に受け取ろうとする人がいます。

そのため、電子データの受け渡しで送信者と受信者以外に情報の漏えいを防ぐため、情報を暗号化することで、第三者に内容が分からないよう対策が行われています。

では、ここで簡単な暗号の例を見ていきましょう。

問題 暗号文「JHSZJT」は何を意味しているか。

これは、伝えたい英単語のアルファベットを1つ前の文字で置き換えて作った暗号です。

つまり、解読に必要な規則は「1つ後のアルファベットに置き換えること」(ただし、Zの次はAとする)であり、Jの次はKと順に変換すれば、答えは「KITAKU」と解読できます。

ここでは、暗号の作成者が暗号化と解読に必要な「規則」(鍵)を皆様に伝えたので、お互い暗号の意味を知ることができました。しかし、この方法で第三者に知られることなく暗号を作成し解読するには、必要な規則を情報の受け取り相手だけに伝えるため、直接会って言うなど何らかの工夫が必要です。

そこで、上記の弱点を改善した「RSA暗号」が開発されました。

RSA暗号では、情報の受信者が「暗号化するための規則」(公開鍵)と「解読するための規則」(秘密鍵)を別々に作成し、公開鍵だけを公開します。

そして、情報の送信者は公開鍵で伝えたい内容を暗号化して送り、受信者は自分だけが知っている秘密鍵で暗号を解読します。また、「公開鍵」「秘密鍵」の作成には、2つの大きな素数とそれらを掛けた数を用います。

これは、大きな数を素数の掛け算の形で表すことが難しい性質を利用するためです。

生誕100年を迎えた日本文学の伝道師ドナルド・キーン氏の生年月日は1922年6月18日ですが、この数字を後ろから並べなおした「8162291」という数を考えてみましょう。

問題 「8162291」は2つの素数の掛け算でどう表せるか。

この問題の答えは、 $8162291 = 2357 \times 3463$ となりますが、すぐに見つけるのは難しかったのではないのでしょうか。

実際は、これより遥かに大きな数が使われており、人間はおろかコンピューターでも導き出すのに膨大な時間を要します。

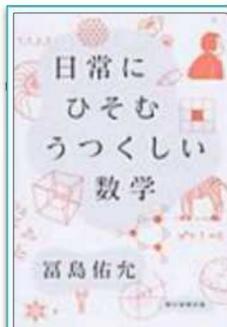
そのため、第三者が公開鍵を知ることができても、暗号の解読に必要な秘密鍵を導くことは非常に困難でありRSA暗号の安全性が保たれています。

北区立図書館は、こうした日常にまつわる意外な知識の宝庫です。

皆さまのご来館をぜひお待ちしております。

3月休館日のご案内

3月1日(水)・2日(木)…特別整理日のため
昭和田・上十条・赤羽北図書館休館
3月6日(月)・20日(月)…中央図書館休館
毎週月曜日……………中央図書館以外の図書館休館
3月31日(金)…館内整理日のため全館休館



中央図書館所蔵参考図書

★『日常にひそむ うつくしい数学』

富島 佑允/著 朝日新聞出版

私たちは数学とともに生きている。この世界を数学的な視点で見よう。「かたち」「かず」「うごき」などをテーマに、身の回りにある様々な「不思議」「美しい」「おもしろい」に隠された法則を、数学を使って解き明かす。

お知らせ

新着図書

3月の

図書館で読書会

参加者同士で課題本についての感想を話し合います。

課題本『宝さがしの子どもたち』

E・ネズビット/作

よしだしんいち 吉田新一/訳 スーザン・アインツヒ/画

福音館書店

日時：3月4日（土）

午後1時30分～3時

場所：中央図書館3階ホール

申込：不要。当日、直接会場へ

問合せ先：中央図書館事業係

☎ (5993)1125



フックスタートフォローアップ事業

ちびっこ絵本サロン

企画・運営 北区図書館活動区民の会

手遊び、絵本、季節の遊びを楽しみます。

対象：1～2歳のお子さんと保護者

日時：3月19日（日）

午前10時45分

※受付10時30分頃から

場所：旧いなり公園（十条台1-2）

※中央図書館前の芝生広場先

※ご不明な点は、右記QRコードから

本事業のホームページでもご確認いただけます。

※天候が悪い場合は、中央図書館3階ホール

（十条台1-2-5）で実施のため、

当日、先着6組となります。

定員：10組程度（当日、先着順）

申込：不要。当日、直接会場へ

問合せ先：中央図書館事業係 ☎ (5993)1125



ご利用ください

手話サポートデスク

日時：3月18日（土）

午後1時～3時

場所：中央図書館1階

総合カウンターにお声かけください。

※図書館利用でお困りのことや

福祉機器などの説明を手話（筆談）

通訳します。



開催事業につきましては、新型コロナウイルス感染拡大状況により、内容変更や中止・延期となる場合がございます。あらかじめご了承ください。

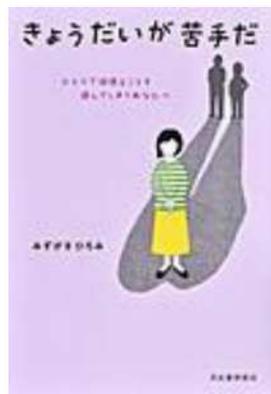


★『教養のある人がしている、

言葉選びの作法』

さいとうなほ 齋藤孝/著 ぱる出版

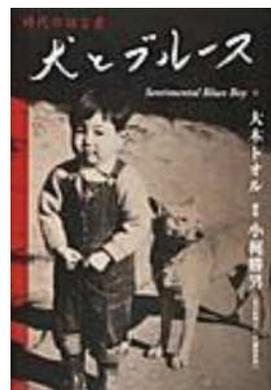
誰もがアウトプットを求められる SNS 全盛時代において、言葉のセンスをいかに磨くか。「センスがある」「一味違う」と思われる言葉の正体を丁寧に解きほぐし、その習得の仕方を解説する。



★『きょうだいが苦手だ』

みずがきひろみ/著 河出書房新社

連絡が途切れると「何か、悪いことした？」と焦る、「なぜ私ばかり」と感じることが多い…。イライラ、モヤモヤの背後には「きょうだいとの競争」があった。人間関係が180度変わる「きょうだい」克服メソッドを伝授する。



★『犬とブルース』

おおき 大木トオル/著 鳥影社

アメリカ合衆国に唯ひとり戦いを挑んだブルースシンガーであり、動物愛護法の改正に尽力するセラピードッグのパイオニア、大木トオルの魂の物語。『読売新聞』連載とインタビューをもとに書籍化。



★『正解のない世の中を生きる』

はやまじゅん 葉山潤奈/著 ワニブックス

人生で最も大きな損失は、心の中で何かが死んでしまうこと。愛に振り回されないセルフブランディングで心を守る！ 人気インフルエンサーが、誹謗中傷、SNS いじめで負った傷の手放し方を伝授する。

3月テーマ展示 (注) 休館日を除く

図書館	一般	児童
中央	【1階総合フロア】 春うらら	ほかほか 
	【北区の部屋】 昭和57年浮間 —図書館員たちが残した記録写真—	
中央分室	いつもありがとう	おともだち
上十条	時代小説	耳(みみ)
豊島	花と緑をたのしもう	えほんのえのせかい
東十条		はな
赤羽	SNSのあれこれ	どうぶつといっしょ
浮間	初めてを始めよう	はるをさがそう
赤羽西		おすすめ
赤羽北	趣味を見つけよう!!	ともだちっていいね!
神谷	ねがう	ねがう
滝野川	エシカル消費 —わたしたちにできること—	みんなで あそぼう
昭和町	スタート	どんなかお?
田端	【一般】 プロフェッショナル	いどうする 
	【田端文士村】 田端文士村の芸術 ～工芸を中心に～	
東田端	住まいを整える	大きくなったよ
滝野川西	DIYで大改造	カラフル

滝野川図書館 3月の展示本

テーマ: 「エシカル消費-わたしたちにできること-」

お買い物はマイバッグ、食べ残しをなくすなど個人でも気軽に環境や社会のためにできることがあるエシカル消費。ちょっと地球にいいことはじめてみませんか?

▼『SDGs時代の食べ方』

井出留美/著
筑摩書房



▼『暮らしのなかのSDGs』

アノニマ・スタジオ/編
KTC中央出版



▲『これってホントにエコなの?』
ジョージナ・ウィルソン=パウエル/著
吉田綾/監訳
吉原かれん/訳
東京書籍



▲『サルベージ・パーティから生まれた「使い切る」ための4つのアイデアと50のレシピ』
キムラカズヒロ/著
フードサルベージ/監修
成文堂新光社



▲『SDGsな生活のヒント』
タラ・シャイン/著
たけいまり
武井摩利/訳
創元社

行事案内リスト

リサイクル ※在庫がなくなり次第終了。【雑】は雑誌、【図】は図書

滝野川	3/11(土)[雑] 3/25(土)[図] 4/8(土)[雑] 4/22(土)[図]
昭和町	3/11(土)[雑] 3/25(土)[図] 4/8(土)[雑] 4/22(土)[図]
田端	3/11(土)[雑] 3/25(土)[図] 4/8(土)[雑] 4/22(土)[図]
東田端	3/11(土)[雑] 3/25(土)[図] 4/8(土)[雑] 4/22(土)[図]
滝野川西	3/11(土)[雑] 3/25(土)[図] 4/8(土)[雑] 4/22(土)[図]

左記以外の館については、リサイクル資料の準備ができたタイミングで提供しています。
特定の日、曜日、時間での提供はしていません。

幼児向けおはなし会など

中央	3/18、25(土)午前11時
	3/18(土)午後3時(小学生向け)
	3/25(土)午後2時30分(紙芝居)
浮間	3/7、14、28(火)午前11時
	3/24(金)午後3時30分
上十条	3/8(水)午後3時50分
赤羽北	3/9(木)、3/24(金)午前11時
豊島	3/16(木)午前10時

赤ちゃんのためのおはなし会

中央	3/18(土)午前10時
	3/27(月)午前11時10分
中央分室	3/19(日)午前11時
滝野川	3/17(金)午前11時
赤羽	3/8(水)午前10時30分
田端	3/3、24(金)午前11時
上十条	3/8(水)午前11時
神谷	3/9(木)午前11時
豊島	3/16(木)午前10時40分
東十条	3/17(金)午前11時10分

おはなし会については
右記QRコードからも
ご確認いただけます。



行事内容は、新型コロナウイルスの感染状況により
変更になる場合があります。ご理解、ご協力をお願いいたします。

予約多数リスト

一般図書編

令和5年2月15日時点(予約状況は毎日変動しています)

位	予約数	タイトル・著者等・出版元	所蔵数
1	578	おいしいごはんが食べられますように 高瀬隼子／著 講談社	17
2	509	同志少女よ、敵を撃て 逢坂冬馬／著 早川書房	19
3	504	ジェyson流お金の増やし方 厚切りジェyson／著 ぴあ	9
4	453	#真相をお話しします 結城真一郎／著 新潮社	12
5	407	夜に星を放つ 窪美澄／著 文藝春秋	15
6	387	三千円の使いかた 原田ひ香／著 中央公論新社	15
7	338	マスカレード・ゲーム 東野圭吾／著 集英社	15
8	335	世界の「頭のいい人」がやっていることを1冊にまとめてみた 中野信子／著 アスコム	7
9	327	六人の嘘つきな大学生 浅倉秋成／著 KADOKAWA	17
10	301	ハヤブサ消防団 池井戸潤／著 集英社	12

CD編

位	予約数	タイトル・アーティスト・発売元	所蔵数
1	139	BOOTLEG 米津玄師 SONY Records	2
2	107	STRAY SHEEP 米津玄師 SME Records	2
3	103	Traveler Official 髭男dism ポニーキャニオン	2
4	84	Editorial Official 髭男dism IRORI Records ／ポニーキャニオン／ラストラム	2
5	76	BADモード 宇多田ヒカル EPIC	2
6	74	おいしいパスタがあると聞いて あいみょん unBORDE	2
6	74	LOVE ALL SERVE ALL 藤井風 HEHN RECORDS	2
8	73	瞬間的シックスセンス あいみょん unBORDE	2
9	62	diorama 米津玄師 REISSUE RECORDS inc.	2
10	61	CEREMONY King Gnu アリオラジャパン	2