



Vídeos da TV Escola

DICAS PEDAGÓGICAS

Matemática em Toda Parte II

Episódio: “Matemática na Comunicação”

Resumo

O episódio “Matemática na Comunicação” aborda como a Matemática tem ajudado o homem a se comunicar, revelando o que está oculto nas mensagens e escondendo aquilo que não pode ser revelado. No primeiro bloco são apresentadas situações envolvendo a construção de mensagens por meio de códigos criados pelo homem no Egito antigo, como a Pedra de Roseto, e nos dias atuais, com a codificação da artista plástica Joana Cesar, mostrando como a Criptografia usa a Matemática para cifrar e decifrar mensagens. O segundo bloco vai investigar a Matemática por trás da comunicação digital e, para isso, mostrará o outro lado da Criptografia: ajudar a esconder o que não pode ser revelado, como as senhas bancárias, ordens de compra e venda, projetos empresariais e uma série de outras informações que precisam ser guardadas em segurança. Temas como os números primos, divisibilidade, análise e explosão combinatória são abordados nesse bloco. Uma excelente oportunidade para conhecer relações entre a Matemática e a linguagem, principalmente as presentes no mundo digital. Boa conexão!

Palavras-chave

Comunicação digital, criptografia, *internet*, números primos.

Nível de ensino

Ensinos Fundamental e Médio.

Componente curricular

Matemática.

A TV Escola leva até a sua sala de aula os melhores documentários e séries de conteúdo educativo. Acompanhe nossa programação no **Canal 123 da Embratel**, no **Canal 112 da SKY**, no **Canal 694 da Telefônica TV Digital** ou gratuitamente sintonizando sua **antena parabólica: analógica - Hor /Freq. 3770 e digital banda C Vert /Freq. 3965**

Na internet acesse <http://tvescola.mec.gov.br> e assista ao vivo, 24 horas.



Vídeos da TV Escola

DICAS PEDAGÓGICAS

Disciplinas relacionadas

Língua Portuguesa, História e Sociologia.

Aspectos relevantes do vídeo

- ❖ Mostrar como a Matemática está relacionada às diferentes formas de enviar mensagens, ajudando na construção, decifração e ocultação das informações contidas em tais mensagens.
- ❖ Mostrar que a necessidade do envio de mensagens secretas está presente em diversas culturas, do Egito antigo ao mundo tecnológico atual, em que as técnicas de transmissão dessas mensagens estão intimamente ligadas a conceitos matemáticos.
- ❖ Abordar as ideias básicas da Criptografia de forma simples e acessível ao nível de conhecimento matemático de alunos da Educação Básica.
- ❖ Mostrar que números primos e divisibilidade formam a base da segurança e do sigilo de muitas informações transmitidas via *internet*, incluindo aí senhas, informações bancárias, imagens, vídeos e áudios nas redes sociais etc., tão comuns e próximas a essa nova geração que vive no século XXI.
- ❖ Associar Matemática ao mundo digital: só é possível viver o virtual graças a muita Matemática, desde conceitos simples e acessíveis aos alunos, a conceitos complexos, possíveis apenas aos especialistas.
- ❖ Discutir a construção de senhas mais seguras por meio da análise combinatória.

Duração da atividade

Duas horas-aula (90 min), cada atividade.

A TV Escola leva até a sua sala de aula os melhores documentários e séries de conteúdo educativo. Acompanhe nossa programação no **Canal 123 da Embratel**, no **Canal 112 da SKY**, no **Canal 694 da Telefônica TV Digital** ou gratuitamente sintonizando sua **antena parabólica: analógica - Hor /Freq. 3770 e digital banda C Vert /Freq. 3965**.
Na internet acesse <http://tvescola.mec.gov.br> e assista ao vivo, 24 horas.



Vídeos da TV Escola

DICAS PEDAGÓGICAS

O que o aluno poderá aprender com esta aula

Utilizar propriedades dos números inteiros para decifrar mensagens.

Utilizar análise combinatória para investigar, construir e classificar processos criptográficos, incluindo as senhas numéricas e alfanuméricas.

Conhecimentos prévios que devem ser trabalhados pelo professor com o aluno

Números primos, múltiplos e divisores.

Porcentagem.

Princípio Fundamental da Contagem e Combinações Simples.

Estratégias e recursos da aula/descrição das atividades

Caro(a) professor(a), apresentaremos algumas sugestões de atividades para dar suporte à exibição do episódio “*Matemática na Comunicação*”. Nossa proposta de atividades foi organizada em duas aulas:

Decifrando Códigos (Ensino Fundamental)

Combinatória e Criptografia (Ensino Médio)

O planejamento das aulas buscou articular o conteúdo apresentado no vídeo às atividades propostas. Sugerimos que a primeira aula seja realizada no Ensino Fundamental (6º ao 8º ano), e a segunda aula aplicada no Ensino Médio, ao longo do estudo da Análise Combinatória. Para facilitar a adequação dessa proposta à realidade de cada professor, apresenta-se a duração das atividades.

As atividades de cada uma das aulas foram postas em páginas individuais exclusivas, separadas do restante do texto para serem impressas e utilizadas em sala de aula, aqui denominadas Folha de Atividades. Imediatamente após cada Folha de Atividades são apresentados comentários e sugestões para auxiliarem na aplicação em sala de aula.

A TV Escola leva até a sua sala de aula os melhores documentários e séries de conteúdo educativo. Acompanhe nossa programação no **Canal 123 da Embratel**, no **Canal 112 da SKY**, no **Canal 694 da Telefônica TV Digital** ou gratuitamente sintonizando sua **antena parabólica: analógica - Hor /Freq. 3770 e digital banda C Vert /Freq. 3965**

Na internet acesse <http://tvescola.mec.gov.br> e assista ao vivo, 24 horas.



Vídeos da TV Escola

DICAS PEDAGÓGICAS

Professor(a), este material foi elaborado com cuidado de modo que sua aplicação seja factível, mas lembre-se de que essas sugestões podem e devem ser adaptadas à sua realidade.

Aula 1: Decifrando códigos

Antes de começarmos a atividade, vamos ampliar a visão sobre a Criptologia. Utilizaremos dois textos sobre o assunto, voltados para os Ensinos Fundamental e Médio, presentes no currículo do Programa de Iniciação Científica da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP).

Enviar mensagens secretas é uma tarefa muito antiga, nascida com a diplomacia e com as transações militares. Em grego, *cryptos* significa secreto, oculto. A Criptografia estuda os métodos para codificar uma mensagem de modo que apenas o seu destinatário legítimo consiga interpretá-la. É a arte dos “códigos secretos”. O uso de códigos secretos costuma estar presente até em brincadeiras de crianças.

Hoje em dia, com as comunicações no mundo digital, muitas atividades dependem do sigilo na troca de informações, incluindo aí as transações financeiras, militares e corporativas, dentre outras. A ciência que estuda sistemas de envio e recepção de mensagens secretas chama-se *Criptologia*, e se divide em três áreas:

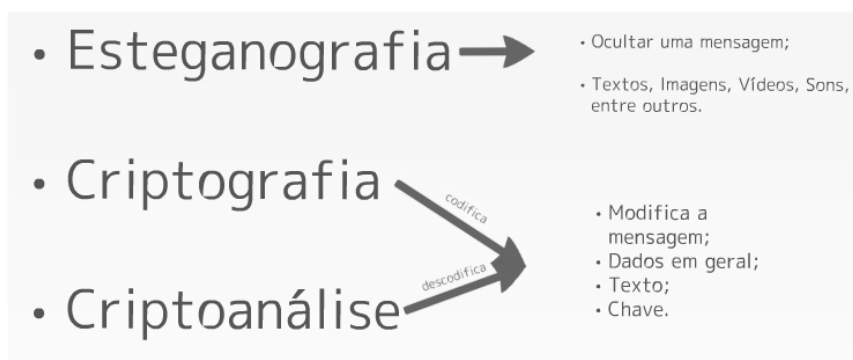


Figura 1 – Divisão da Criptologia.

Fonte: <<http://prezi.com/wbsxqlvw-oso/criptologia-bcc-2010>>

A TV Escola leva até a sua sala de aula os melhores documentários e séries de conteúdo educativo. Acompanhe nossa programação no **Canal 123 da Embratel**, no **Canal 112 da SKY**, no **Canal 694 da Telefônica TV Digital** ou gratuitamente sintonizando sua **antena parabólica: analógica - Hor /Freq. 3770 e digital banda C Vert /Freq. 3965**.
Na internet acesse <http://tvescola.mec.gov.br> e assista ao vivo, 24 horas.



Vídeos da TV Escola

DICAS PEDAGÓGICAS

Esse envio, codificação, decodificação e recebimento de mensagens está simplificada e representado a seguir:

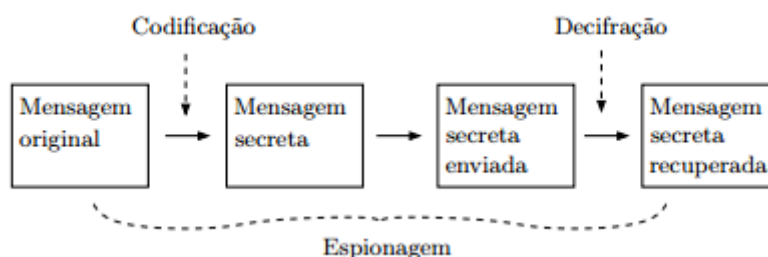


Figura 2 – Esquema do processo de codificação, envio e decodificação de uma mensagem.

Fonte: <http://www.obmep.org.br/prog_ic_2010/apostila2010.html>

O objetivo das próximas atividades é decifrar códigos utilizando diferentes técnicas.

1º Momento: Preparação da apresentação do vídeo (10 minutos)

Inicialmente, divida a turma em duplas. Em seguida, inicie uma conversa rápida dizendo que nesta aula serão realizadas atividades envolvendo decifração de códigos.

2º Momento: Exibição completa do vídeo (20 minutos)

Exiba o programa completo. Além dos quase quinze minutos de duração do vídeo, foram adicionados cinco minutos para considerações finais antes da aplicação da Folha de Atividades.

3º Momento (60 minutos)

Aplicação da Folha de Atividades com questões cujas respostas serão registradas na folha, pelos alunos. Sugerimos fortemente que os alunos tentem resolver os problemas a partir de suas próprias estratégias. Caberá ao professor decidir se primeiramente introduzirá os conceitos, seguindo com exemplos, para depois partir para os problemas; ou se construirá os conceitos juntamente com a resolução dos problemas.

A TV Escola leva até a sua sala de aula os melhores documentários e séries de conteúdo educativo. Acompanhe nossa programação no **Canal 123 da Embratel**, no **Canal 112 da SKY**, no **Canal 694 da Telefônica TV Digital** ou gratuitamente sintonizando sua **antena parabólica: analógica - Hor /Freq. 3770 e digital banda C Vert /Freq. 3965**

Na internet acesse <http://tvescola.mec.gov.br> e assista ao vivo, 24 horas.



Vídeos da TV Escola

DICAS PEDAGÓGICAS

Folha de Atividades – Aula 1

Decifrando Códigos

Atividade 1

Um dos primeiros sistemas de Criptografia conhecido foi elaborado pelo general Júlio César, no Império Romano. Júlio César substituiu cada letra pela terceira letra que a segue no alfabeto.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Q	R	S	T	U	V	W	X	Y	Z						
T	U	V	W	X	Y	Z	A	B	C						

Figura 3 – Sistema Criptográfico de Júlio César.

Baseado nesse critério:

- Codifique a frase: Eu gosto de Matemática.
HX JRVWR GH PDWHPDWLFD.
- Decifre a mensagem OHJDO FRQVHJXL.
LEGAL CONSEGUI.

Em vez de caminhar três letras para frente, podemos andar outro número de letras e teremos um novo método de cifrar mensagens. Esse número é chamado de chave ou senha do sistema criptográfico, o qual, por motivos óbvios, só deve ser conhecido por quem envia a mensagem e por quem a recebe.

A TV Escola leva até a sua sala de aula os melhores documentários e séries de conteúdo educativo. Acompanhe nossa programação no **Canal 123 da Embratel**, no **Canal 112 da SKY**, no **Canal 694 da Telefônica TV Digital** ou gratuitamente sintonizando sua **antena parabólica: analógica - Hor /Freq. 3770 e digital banda C Vert /Freq. 3965**
Na internet acesse <http://tvescola.mec.gov.br> e assista ao vivo, 24 horas.



Vídeos da TV Escola

DICAS PEDAGÓGICAS

Estabeleça agora o seu critério de codificação avançando mais do que três letras. Escreva uma palavra para a outra pessoa da sua dupla e peça a ela para tentar decodificar sua mensagem. Se ela não conseguir, conte o seu critério e peça para ela tentar novamente.

Atividade 2

Podemos transformar letras em números, no processo de substituição de letras para criptografar uma mensagem. No quadro abaixo, temos um exemplo de como podemos fazer essa associação.

A=0	B=1	C=2	D=3	E=4	F=5	G=6	H=7
I=8	J=9	K=10	L=11	M=12	N=13	O=14	P=15
Q=16	R=17	S=18	T=19	U=20	V=21	W=22	X=23
Y=24	Z=25						

Figura 4 – Sistema Criptográfico associando letras a números.

Desse modo, a letra codificada é obtida da letra original, somando-se três ao número correspondente. Mas, como vimos, podemos somar outros números. A partir dessas informações, resolva o problema a seguir.

Um antigo método para codificar palavras consiste em escolher um número de 1 a 26, chamado *chave* do código, e girar o disco interno do aparelho ilustrado na figura até que essa chave corresponda à letra A. Depois disso, as letras da palavra são substituídas pelos números correspondentes, separados por tracinhos. Por exemplo, na figura ao lado a chave é 5 e a palavra *PAI* é codificada como 20-5-13.



(a) Usando a chave indicada na figura, descubra qual palavra foi codificada como 23-25-7-25-22-13.

(b) Codifique *OBMEP* usando a chave 20.

(c) Chicó codificou uma palavra de 4 letras com a chave 20, mas esqueceu-se de colocar os tracinhos e escreveu 2620138. Ajude o Chicó colocando os tracinhos que ele esqueceu e depois escreva a palavra que ele codificou.

(d) Em uma outra chave, a soma dos números que representam as letras A, B e C é 52. Qual é essa chave?

A TV Escola leva até a sua sala de aula os melhores documentários e séries de conteúdo educativo.

Acompanhe nossa programação no **Canal 123 da Embratel**, no **Canal 112 da SKY**, no **Canal 694 da Telefônica TV Digital** ou gratuitamente sintonizando sua **antena parabólica: analógica - Hor /Freq. 3770 e digital banda C Vert /Freq. 3965**

Na internet acesse <http://tvescola.mec.gov.br> e assista ao vivo, 24 horas.



Vídeos da TV Escola

DICAS PEDAGÓGICAS

Comentários e soluções

Atividade 1

a) Codifique a frase: Eu gosto de Matemática.

HX JRVWR GH PDWHPDWLFD.

b) Decifre a mensagem OHJDO FRQVHJXL.

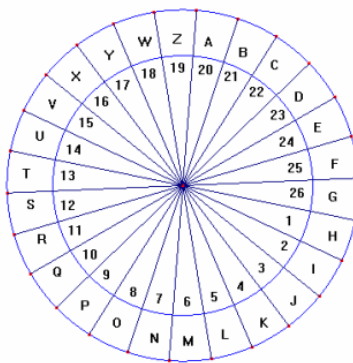
LEGAL CONSEGUI.

A segunda parte dessa atividade gera respostas pessoais dos alunos, dependendo da senha que escolherem.

Atividade 2

(a) A partir da figura do enunciado temos 23=S, 25=U, 7=C, 22=R e 13=I. Logo, a palavra codificada como 23-25-7-25-22-13 é SUCURI.

(b) Para a chave 20 temos a figura abaixo, na qual vemos que O=8, B=21, M=6, E=24 e P=9.



Assim, a codificação de OBMEP é 8-21-6-24-9. Alternativamente, ao passar da chave 5 para a chave 20 devemos somar 15 aos números da figura do enunciado, lembrando que se a soma for maior do que 26 devemos subtrair 26.

A TV Escola leva até a sua sala de aula os melhores documentários e séries de conteúdo educativo. Acompanhe nossa programação no **Canal 123 da Embratel**, no **Canal 112 da SKY**, no **Canal 694 da Telefônica TV Digital** ou gratuitamente sintonizando sua **antena parabólica: analógica - Hor /Freq. 3770 e digital banda C Vert /Freq. 3965**

Na internet acesse <http://tvescola.mec.gov.br> e assista ao vivo, 24 horas.



Vídeos da TV Escola

DICAS PEDAGÓGICAS

Assim, temos:

$$O = 19 + 15 - 26 = 34 - 26 = 8, B = 6 + 15 = 21, M = 17 + 15 - 26 = 6, \\ E = 9 + 15 = 24, P = 20 + 15 - 26 = 9$$

em que OBMEP é codificada como 8-21-6-24-9.

(c) Como não existe letra codificada como 0, um dos números associados a letras na sequência 2620138 é o 20. À sua direita há três dígitos, mas como não há letra codificada como 138 ou 38, os números associados a letras são o 13 e o 8. Isto dá um total de três letras. Portanto, à esquerda de 20 só podemos admitir o 26. Logo, a codificação da palavra é 26-20-13-8, a qual, na chave 20, corresponde a GATO.

(d) Quando somamos três números consecutivos, obtemos um número divisível por 3; por exemplo, $14 + 15 + 16 = 45$. Ao somar os números que representam as letras A, B e C nessa certa chave, obtemos 52, que não é um número divisível por 3. Isso mostra que os três números não são consecutivos e isso somente é possível se um dos números for 26 e outro for 1. Como a soma é 52, o terceiro número é $52 - 27 = 25$. A única codificação de ABC, nesse caso, é 25-26-1, ou seja, a chave é 25.

A TV Escola leva até a sua sala de aula os melhores documentários e séries de conteúdo educativo. Acompanhe nossa programação no **Canal 123 da Embratel**, no **Canal 112 da SKY**, no **Canal 694 da Telefônica TV Digital** ou gratuitamente sintonizando sua **antena parabólica: analógica - Hor /Freq. 3770 e digital banda C Vert /Freq. 3965**
Na internet acesse <http://tvescola.mec.gov.br> e assista ao vivo, 24 horas.



Vídeos da TV Escola

DICAS PEDAGÓGICAS

Aula 2: Combinatória e Criptografia

As atividades da Aula 2 têm como objetivo aplicar técnicas básicas de contagem no contexto da Criptografia. Temas como princípio multiplicativo, permutações, combinações, e desordenamentos são abordados em situações em processos de codificação e construção de mensagens e senhas. Apresenta-se também como a análise combinatória pode ajudar a quantificar o número de senhas e sua relação com a segurança destas.

É muito importante que os alunos já tenham visto o princípio multiplicativo, também chamado de princípio fundamental da contagem.

1º Momento: Preparação da apresentação do vídeo (10 minutos)

Inicialmente, divida a turma em duplas. Em seguida, inicie uma conversa rápida dizendo que nesta aula serão realizadas atividades envolvendo Análise Combinatória e Criptografia.

2º Momento: Exibição completa do vídeo (20 minutos)

Exiba o programa completo. Além dos quase quinze minutos de duração do vídeo, foram adicionados cinco minutos para considerações finais antes da aplicação da Folha de Atividades.

3º Momento (60 minutos)

Aplicação da Folha de Atividades com questões cujas respostas serão registradas na folha, pelos alunos. Sugerimos fortemente que os alunos tentem resolver os problemas presentes nas atividades a partir de suas próprias estratégias. Cabe ao professor auxiliar o trabalho dos alunos quando julgar necessário, buscando intervir sem retirar o prazer da descoberta.

A TV Escola leva até a sua sala de aula os melhores documentários e séries de conteúdo educativo. Acompanhe nossa programação no **Canal 123 da Embratel**, no **Canal 112 da SKY**, no **Canal 694 da Telefônica TV Digital** ou gratuitamente sintonizando sua **antena parabólica: analógica - Hor /Freq. 3770 e digital banda C Vert /Freq. 3965**

Na internet acesse <http://tvescola.mec.gov.br> e assista ao vivo, 24 horas.



Folha de Atividades – Aula 2

Combinatória e Criptografia

Atividade 1

Na sequência de perguntas a seguir, usaremos técnicas de análise combinatória no contexto da Criptografia, investigando processos de codificação de mensagens.

Um dos primeiros sistemas de Criptografia conhecido foi elaborado pelo general Júlio César, no Império Romano. Júlio César substituiu cada letra pela terceira letra que a segue no alfabeto.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Q	R	S	T	U	V	W	X	Y	Z						
T	U	V	W	X	Y	Z	A	B	C						

Figura 5 – Quadro de substituição do sistema de Júlio Cesar.

Em vez de caminhar três letras para frente, podemos andar outro número de letras pra frente, de modo a substituir cada letra pela *n*ésima letra que a segue no alfabeto. Esse número é chamado de chave ou senha do sistema criptográfico, o qual, por motivos óbvios, só deve ser conhecido por quem envia a mensagem e por quem a recebe. Esse método é dito semelhante ao de Júlio César.

- 1) Nos sistemas que seguem um princípio semelhante ao de Júlio César, quantas chaves diferentes podem ser usadas para obter configurações diferentes?



Consideremos agora um país ALFA, onde apenas três letras são utilizadas: A, B e C.

- 2) Preencha os quadros abaixo exibindo todas as possibilidades de criptografar mensagens.

1	2	3
A	B	C

1	2	3
A	B	C

1	2	3
A	B	C

1	2	3
A	B	C

1	2	3
A	B	C

1	2	3
A	B	C

1	2	3
A	B	C

- 3) Dessas formas, qual delas não codifica nada?
4) Sem listar, como poderíamos calcular que existem seis delas? E se fossem n letras diferentes?
5) Apresente as formas em que há “desordenamento”, ou seja, em que nenhuma letra está em sua posição original.

Considere agora um país BETA, em que são utilizadas quatro letras: A, B, C e D.

- 6) Quantas palavras diferentes existem, usando as quatro letras?
7) Liste as 24 palavras possíveis usando os quadros a seguir.

1	2	3	4
A	B	C	D

2	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D



1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

1	2	3	4
A	B	C	D

- 8) Das 24 palavras possíveis, quantas delas respeitam a ordem usual e quais são elas?
9) Quantos e quais são os desordenamentos?

Para encerrar a atividade, mais um pouco de combinatória no mundo das senhas.

- 10) Quantas senhas de seis caracteres podemos formar usando apenas os 10 algarismos do sistema decimal?
11) E se fossem apenas as 26 letras do alfabeto?
12) E se fosse possível usar as 26 letras e os 10 algarismos?
13) Qual o aumento percentual do número de senhas possíveis do item 11 para o item 13?
14) Se um computador fosse capaz de verificar 1 milhão de senhas por segundo, quanto tempo levaria para verificar todas as senhas possíveis do item 11?
15) Faça o mesmo para os itens 12 e 13, e compare os tempos encontrados.



Comentários e soluções

Atividade 1

- 1) 25 formas diferentes, pois 0 e 26 não contam nada.
- 2) Preencha a tabela abaixo exibindo todas as possibilidades de criptografar mensagens.

1	2	3
A	B	C
1	2	3
A	B	C

1	2	3
A	B	C
1	3	2
A	C	B

1	2	3
A	B	C
2	1	3
B	A	C

1	2	3
A	B	C
2	3	1
B	C	A

1	2	3
A	B	C
3	1	2
C	A	B

1	2	3
A	B	C
3	2	1
C	B	A

- 3) Dessas formas, qual delas não codifica nada?
A primeira forma: ABC é igual ao real, portanto não codifica.
- 4) Sem listar, como poderíamos calcular que existem seis delas? E se fossem n letras diferentes?
Usando o princípio multiplicativo, temos $3 \cdot 2 \cdot 1 = 6$ possibilidades.
Para n letras, temos: $n \cdot (n-1) \cdot (n-2) \dots 3 \cdot 2 \cdot 1$. Esse produto é conhecido como fatorial de n e é pode ser representado por “n!”.
- 5) Apresente as formas em que há “desordenamento”, ou seja, em que nenhuma letra está em sua posição original.
BCA e CAB. Ou ainda, 231 e 312.
Esse exemplo é bem fácil de contar um a um. Pode-se chegar ao resultado sem precisar listar todas as formas.
Ao todo temos três! = 6 possibilidades.
Considere os seguintes conjuntos:
A: conjunto das sequências que possuem o A no seu lugar de origem.



Vídeos da TV Escola

DICAS PEDAGÓGICAS

B: conjunto das sequências que possuem o B no seu lugar de origem.

C: conjunto das sequências que possuem o C no seu lugar de origem.

Se contarmos o número de elementos do conjunto $A \cup B \cup C$, ou seja, $n(A \cup B \cup C)$, teremos o total de sequências com alguma letra em sua posição original. Daí bastará subtrair do total de sequências, já calculada, para obtermos o número de sequências que não possuem letra alguma em sua posição original.

$$n(A) = 1.2! = 2 \quad n(B) = 1.2! = 2 \quad n(C) = 1.2! = 2$$

$$n(A \cap B) = 1 \quad n(A \cap C) = 1 \quad n(B \cap C) = 1$$

$$n(A \cap B \cap C) = 1$$

Agora é só calcular $n(A \cup B \cup C)$. Para isso, representaremos os três conjuntos por meio de diagramas e representando o número de elementos de cada região possível entre os três conjuntos.

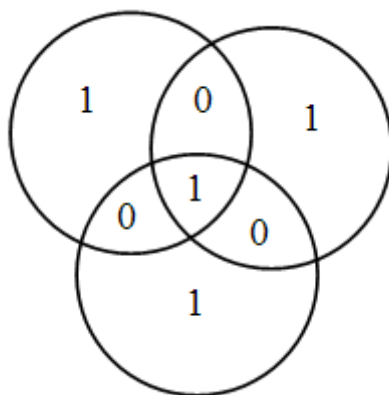


Figura 6 – Diagrama de Venn aplicado ao problema.

Logo, $n(A \cup B \cup C) = 4$ e, portanto, o número de desordenamentos é igual a $6 - 4 = 2$. Observe ainda que, para contarmos os elementos da união entre três conjuntos, começamos somando os elementos de cada conjunto. Ao fazer isso, contamos elementos mais de uma

A TV Escola leva até a sua sala de aula os melhores documentários e séries de conteúdo educativo. Acompanhe nossa programação no **Canal 123 da Embratel**, no **Canal 112 da SKY**, no **Canal 694 da Telefônica TV Digital** ou gratuitamente sintonizando sua **antena parabólica: analógica - Hor /Freq. 3770 e digital banda C Vert /Freq. 3965**

Na internet acesse <http://tvescola.mec.gov.br> e assista ao vivo, 24 horas.



vez. De fato, os elementos das interseções dois a dois foram contados duas vezes. Para corrigir isso, basta subtrair da soma inicial, o número de elementos de cada uma dessas interseções. Mas, com isso geramos um problema, pois a interseção dos três conjuntos foi considerada três vezes, quando fizemos $n(A) + n(B) + n(C)$ e desconsiderada três vezes, quando subtraímos $n(A \cap B)$, $n(A \cap C)$ e $n(B \cap C)$. Para resolver isso, basta somar uma vez $n(A \cap B \cap C)$. Esse raciocínio nos leva à seguinte fórmula:

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - [n(A \cap B), n(A \cap C) \text{ e } n(B \cap C)] + n(A \cap B \cap C).$$

Considere agora um país BETA, em que são utilizadas quatro letras: A, B, C e D.

- 6) Quantas palavras diferentes existem, usando as quatro letras?

Para quatro letras, por exemplo: A, B, C e D. Assim, pelo Princípio Fundamental da Contagem temos $4.3.2.1 = 24$ possibilidades.

- 7) Liste as 24 formas possíveis usando a tabela a seguir.

1	2	3	4
A	B	C	D

2	1	3	4
B	A	C	D

3	1	2	4
C	A	B	D

4	1	2	3
D	A	B	C

1	2	4	3
A	B	D	C

2	1	4	3
B	A	D	C

3	1	4	2
C	A	D	B

4	1	3	2
D	A	C	B

1	3	2	4
A	C	B	D

2	3	1	4
B	C	A	D

3	2	1	4
C	B	A	D

4	2	1	3
D	B	A	C

1	3	4	2
A	C	D	B

2	3	4	1
B	C	D	A

3	2	4	1
C	B	D	A

4	2	3	1
D	B	C	A

1	4	2	4
A	D	B	C

2	4	1	3
B	D	A	C

3	4	1	2
C	D	A	B

4	3	1	2
D	C	A	B

1	4	3	2
A	D	C	B

2	4	3	1
B	D	C	A

3	4	2	1
C	D	B	A

4	3	2	1
D	C	B	A



Vídeos da TV Escola

DICAS PEDAGÓGICAS

8) Das 24 formas possíveis, quantas delas respeitam a ordem usual e quais são elas?

ABCD, BCDA, CDAB, DABC. Temos quatro delas. Obs.: Por ordem usual entende-se aqui a ordem na qual as letras seguem a sequência alfabética, mas tomando-se a letra A como sucessora da letra D.

9) Quantos e quais são os desordenamentos?

Para listar os desordenamentos, podemos usar o quadro construído no item 8. Assim, temos ao todo nove desordenamentos. São eles:

BADC, BDAC, CADB, CDAB, CDBA, DABC, DBAC, DCAB, DCBA.

Esse número já não é tão fácil de contar por enumeração (um a um) quanto o anterior. Entretanto, é possível obter o resultado sem precisar listar todas as formas, utilizando as técnicas básicas de Análise Combinatória.

Ao todo temos quatro! = 24 possibilidades.

Considere os seguintes conjuntos:

A: conjunto das sequências que possuem o A no seu lugar de origem.

B: conjunto das sequências que possuem o B no seu lugar de origem.

C: conjunto das sequências que possuem o C no seu lugar de origem.

D: conjunto das sequências que possuem o D no seu lugar de origem.

Se contarmos o número de elementos do conjunto $A \cup B \cup C \cup D$, ou seja, $n(A \cup B \cup C \cup D)$, teremos o total de sequências com alguma letra em sua posição original. Daí bastará subtrair do total de sequências, que já temos, para obtermos o número de sequências que não possuem letra alguma em sua posição original.

Temos que:

$$n(A) = 3! = 6 \quad n(B) = 3! = 6 \quad n(C) = 3! = 6 \quad n(D) = 3! = 6$$

A TV Escola leva até a sua sala de aula os melhores documentários e séries de conteúdo educativo. Acompanhe nossa programação no **Canal 123 da Embratel**, no **Canal 112 da SKY**, no **Canal 694 da Telefônica TV Digital** ou gratuitamente sintonizando sua **antena parabólica: analógica - Hor /Freq. 3770 e digital banda C Vert /Freq. 3965**

Na internet acesse <http://tvescola.mec.gov.br> e assista ao vivo, 24 horas.



Vídeos da TV Escola

DICAS PEDAGÓGICAS

De modo análogo, todas as $C_4^2 = 6$ interseções dois a dois possuem dois elementos.

De modo análogo, todas as $C_4^3 = 4$ interseções três a três, possuem um elemento.

E a interseção dos quatro conjuntos, apresenta um elemento.

Para contarmos o número de elementos da união entre quatro conjuntos, começamos somando os elementos de cada conjunto. Ao fazer isso, contamos elementos mais de uma vez. De fato, os elementos das interseções dois a dois foram contados duas vezes, uma em cada conjunto. Para corrigir isso, basta subtrair da soma inicial, o número de elementos de cada uma dessas interseções. Mas, com isso geramos um problema, pois a interseção de três conjuntos, por exemplo: A, B e C, foi considerada três vezes, quando fizemos $n(A) + n(B) + n(C)$ e desconsiderada três vezes, quando subtraímos $n(A \cap B)$, $n(A \cap C)$ e $n(B \cap C)$. E isso acontece para os outros grupos de três conjuntos. Para resolver isso, basta somar uma vez os números de cada uma das interseções três a três, e assim por diante.

Em suma, o número de elementos da união é obtido somando os números de elementos de cada conjunto, subtraindo os números de elementos das interseções dois a dois, somando os das interseções três a três, subtraindo os das interseções quatro a quatro etc.

Em nosso problema, temos:

$$n(A \cup B \cup C \cup D) = 6 + 6 + 6 + 6 - 2 - 2 - 2 - 2 - 2 - 2 + 1 + 1 + 1 + 1 - 1 = 15.$$

Logo, temos $24 - 15 = 9$ desordenamentos.

Para o caso geral, o número de desordenamentos de n elementos é dado por:

$$n! \left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + \frac{(-1)^n}{n!} \right)$$

Essa demonstração do caso geral pode ser obtida em Morgado (1991).

A TV Escola leva até a sua sala de aula os melhores documentários e séries de conteúdo educativo. Acompanhe nossa programação no **Canal 123 da Embratel**, no **Canal 112 da SKY**, no **Canal 694 da Telefônica TV Digital** ou gratuitamente sintonizando sua **antena parabólica: analógica - Hor /Freq. 3770 e digital banda C Vert /Freq. 3965**
Na internet acesse <http://tvescola.mec.gov.br> e assista ao vivo, 24 horas.



Vídeos da TV Escola

DICAS PEDAGÓGICAS

Para encerrar a atividade, mais um pouco de combinatória no mundo das senhas.

10) Quantas senhas de seis caracteres podemos formar usando apenas os 10 algarismos do sistema decimal?

$10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 = 1\ 000\ 000$ de senhas.

11) E se fossem apenas as 26 letras do alfabeto?

De modo análogo, temos $26^6 = 308\ 915\ 776$ (\cong 309 milhões de senhas).

12) E se fosse possível usar as 26 letras e os 10 algarismos?

Aí, teríamos $36^6 = 2\ 176\ 782\ 336$ (\cong 2 bilhões de senhas).

13) Qual o aumento percentual do número de senhas possíveis do item 11 para o item 13?

Taxa = $\frac{2\ 176\ 782\ 336}{1\ 000\ 000} - 1 = 217\ 578\ %$. Ou seja, aproximadamente 200 mil por cento.

14) Se um computador fosse capaz de verificar 1 milhão de senhas por segundo, quanto tempo levaria para verificar todas as senhas possíveis do item 10?

1 segundo.

15) Faça o mesmo para os itens 11 e 12, e compare os tempos encontrados.

- Aproximadamente 309 segundos.
- Aproximadamente 2176 segundos.

A TV Escola leva até a sua sala de aula os melhores documentários e séries de conteúdo educativo. Acompanhe nossa programação no **Canal 123 da Embratel**, no **Canal 112 da SKY**, no **Canal 694 da Telefônica TV Digital** ou gratuitamente sintonizando sua **antena parabólica: analógica - Hor /Freq. 3770 e digital banda C Vert /Freq. 3965**

Na internet acesse <http://tvescola.mec.gov.br> e assista ao vivo, 24 horas.



Vídeos da TV Escola

DICAS PEDAGÓGICAS

Questões para discussão

Pesquisar sobre códigos de barras X códigos holográficos: diferenças e potencialidades.

Há testes de primalidade que apresentem resultados em tempo real?

O que é criptografia quântica?

Professor(a), esperamos que esta proposta tenha ampliado suas ideias. Tenha em mente que é totalmente possível mudar o que foi proposto, alterar a ordem, excluir ou incluir perguntas, abordagens, assuntos etc. O mais importante é adequar a proposta à realidade de sua turma. Os nossos e-mails são ivailmuniz@gmail.com e fernandovillar@ufrj.br. Por favor, entre em contato para informar o que achou desta dica pedagógica e se a utilizou em suas aulas. O seu retorno é muito importante para a Rede da TV ESCOLA.

Referências

COUTINHO, S.C. *Criptografia*. Apostila 7 do Programa de Iniciação Científica da OBMEP. Rio de Janeiro: SBM, 2009.

Disponível em: <http://www.obmep.org.br/prog_ic_2010/apostila2010.html>

LIMA, E. L. et al. *A Matemática do Ensino Médio*. Volume 2. Coleção do Professor de Matemática. SBM/IMPA, 2002.

MALAGUTI, P. *Atividades de Contagem a partir da Criptografia*. Apostila 10 do Programa de Iniciação Científica da OBMEP. Rio de Janeiro: SBM, 2009. Disponível em: <http://www.obmep.org.br/prog_ic_2010/apostila2010.html>

MORGADO, A.C.O et al. *Análise Combinatória e Probabilidade*. Coleção do Professor de Matemática. SBM/IMPA, 1991.

Consultores: Ivail Muniz Junior e Fernando Celso Villar Marinho

A TV Escola leva até a sua sala de aula os melhores documentários e séries de conteúdo educativo. Acompanhe nossa programação no **Canal 123 da Embratel**, no **Canal 112 da SKY**, no **Canal 694 da Telefônica TV Digital** ou gratuitamente sintonizando sua **antena parabólica: analógica - Hor /Freq. 3770 e digital banda C Vert /Freq. 3965**

Na internet acesse <http://tvescola.mec.gov.br> e assista ao vivo, 24 horas.