Bem-vindo! As traduções estão em andamento. Se você encontrar conteúdo em inglês, não se preocupe — estamos trabalhando nisso. Relatar outros problemas

(fechar)

Assuntos ▼





Aluno

◆ UMA JORNADA PELA CRIPTOGRAFIA

Cifras

Cifras vs. códigos

Cifra de troca

Lógica binária XOR

XOR e a cifra de chave única

Exploração do XOR

Operadores binários

Feedback

PRÓXIMA SEÇÃO: Criptografia moderna

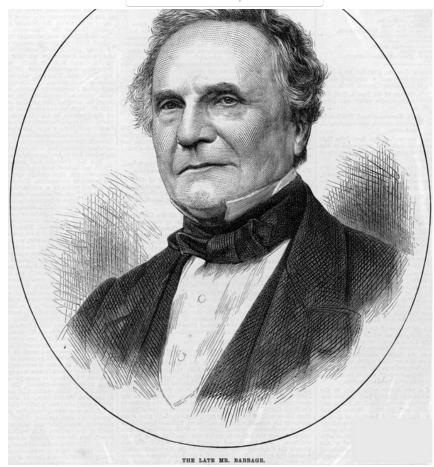
XOR e a cifra de chave única

Por que devemos usar XOR?

Realmente importa se usamos AND, OR ou XOR com cifras de chave única? A resposta é sim e é extremamente importante entender o porquê. Lembre-se do artigo anterior que E tem 75% de chances de retornar 0 e 25% de chances de retornar 1. Enquanto OR tem uma chance de 25% de saída 0 e 75% de chance de saída 1. Enquanto a operação XOR tem 50% de chance de saída 0 ou 1.

Vamos examinar um exemplo visual para ver os diferentes efeitos de embaralhamento de AND, OR e XOR **criptografando uma imagem**. Aqui está uma imagem digital de Charles Babbage: Bem-vindo! As traduções estão em andamento. Se você encontrar conteúdo em inglês, não se preocupe — estamos trabalhando nisso. Relatar outros problemas

(fechar)

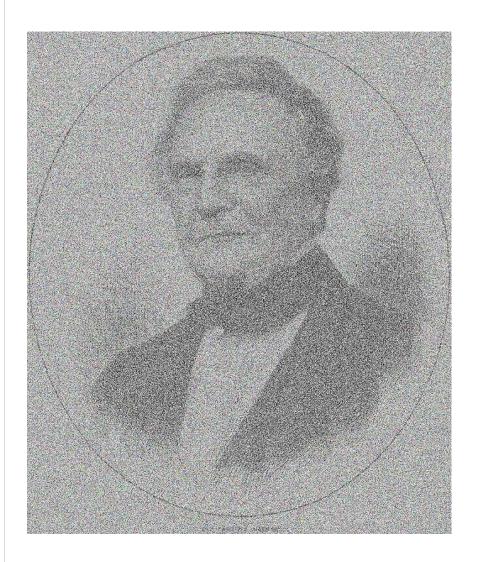


Ela contém milhares de minúsculos quadrados coloridos chamados de pixels. Cada pixel na imagem pode ser representado por uma sequência de 24 bits, conforme mostrado no artigo anterior. Vamos chamá-la de nossa imagem de texto sem formatação (ou mensagem).

Primeiro vamos ver o que acontece quando usamos a operação **E** em cada bit no arquivo da imagem com um fluxo de **bits aleatórios**.

Ε

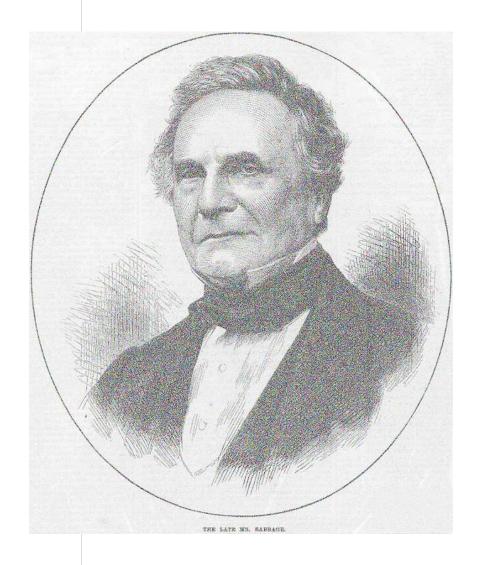
Observe que a maior parte da mensagem original é realçada. Isso acontece sempre que uma troca aleatória de 1 é aplicada, ou quando o texto sem formatação é 0:



Em seguida, vamos ver o que acontece quando usamos o operador **OU** em cada bit do arquivo da imagem com um fluxo de **bits aleatórios**.

OU

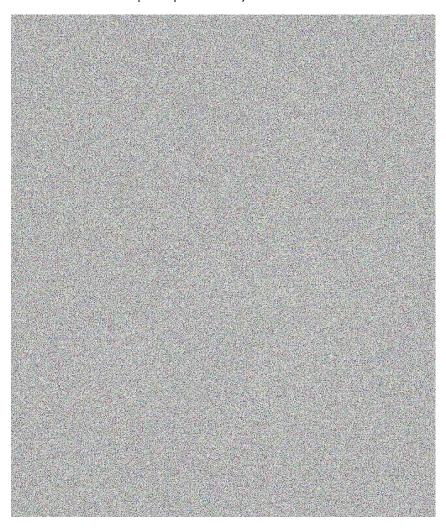
Observe que a maior parte da mensagem original é realçada. Isso acontece quando aplicamos uma troca aleatória de 0, ou quando o texto sem formatação é 1:



Por fim, vamos ver o que acontece quando usamos o operador **XOR** em cada bit do arquivo da imagem com um fluxo de **bits aleatórios**.

(rufem os tambores...)

XOR



Para onde Charles foi?

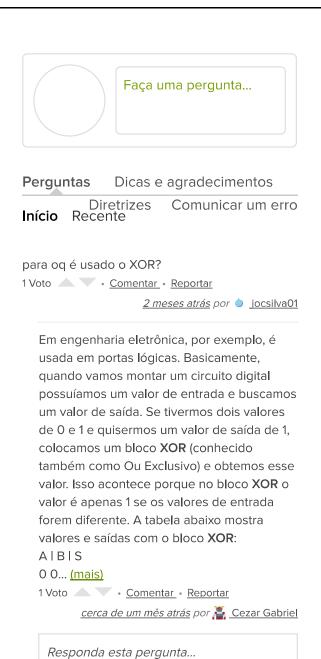
Observe que o texto sem formatação é realçado em apenas **50% do tempo**, o que resulta em <u>ruído</u>, pois cada pixel tem **a mesma probabilidade de ser 0 ou 1**.

Esta imagem não contém <u>nenhuma informação</u> sobre a imagem original. Se nós não fornecêssemos a sequência de troca seria impossível revertê-la de volta à imagem original. Você poderia tentar todas as sequências possíveis, mas elas resultariam em todas as imagens possíveis! Como você saberia que ela era o Babbage? Existe a mesma probabilidade de ser uma foto sua ou de qualquer outra coisa na qual você possa pensar.

Isso não é interessante? Me faz sorrir sempre que vejo isso!

Em seguida, vamos praticar o uso dos operadores XOR, OU e E e <u>descobrir algumas</u> <u>propriedades mais interessantes</u> enquanto isso...

créditos da imagem



Você entende inglês? Clique aqui para ver

mais debates na versão em inglês do site da Khan Academv.

SOBRE	SUPORTE	TUTORIA	CARREIRAS	INTERNACIONAL
Nossa missão Você pode	Central de ajuda	Relatórios de tutor	Trabalho de tempo integral	português ▼ Traduzir nosso conteúdo
aprender qualquer coisa	FALE CONOSCO	Recursos para	Estágios	
Nossa equipe	Contato	Estudos de caso	CONTRIBUA	SOCIAL
Nossos estagiários	I mprensa	Common Core	Faça uma doação	Facebook Twitter
Nossos			Seja voluntário Nossos	Blog
especialistas em conteúdo			apoiadores	A vida na KA
Nossa Diretoria				ACADEMY

Termos de Uso Política de Privacidade

© 2016 Khan Academy

Exceto quando expresso, todos os direitos são reservados.

Aulas e cursos gratuitos para aprendizagem on-line em todos os níveis: fundamental, médio e superior.