Breaking the Caesar Cipher

Introduction

Duke
UNIVERSITY

Breaking Caesar

- You've implemented a Caesar cipher
  - Basic form of encryption, concepts useful
  - We use a key to encrypt, how to decrypt?
- Intended recipient will know the key
  - Encrypt with 7, Decrypt 19
- What about "cracking"?
  - Thief or hacker "finds" key
  - Can we use brute force?

What If a Human Helps?

- Suppose we intercept this message

Lujyfwapvu huk zljbypaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.

- What does this message say?
  - If we knew key to encrypt, we could decrypt
  - How many possible keys are there? Try all!
- Outline of this approach
  - Have code to encrypt, call it with every key
  - Brute force: encryption fast, key space small

Human or Eyeball Decryption

- Unlock or decrypt an encrypted message
  - When we don't have the key

Human or Eyeball Decryption

- Unlock or decrypt an encrypted message
  - When we don't have the key
  - But we do have code for CaesarCipher!

```
public void eyeballDecrypt(String encrypted){
   CaesarCipher cipher = new CaesarCipher();
   for(int k=0; k < 26; k++){
     String s = cipher.encrypt(encrypted,k);
     System.out.println(k+"\t"+s);
   }
}
```

Human or Eyeball Decryption

- Unlock or decrypt an encrypted message
  - When we don't have the key
  - But we do have code for CaesarCipher!

```
public void eyeballDecrypt(String encrypted){
   CaesarCipher cipher = new CaesarCipher();
   for(int k=0; k < 26; k++){
     String s = cipher.encrypt(encrypted,k);
     System.out.println(k+"\t"+s);
   }
}
```

Human or Eyeball Decryption

- Unlock or decrypt an encrypted message
  - When we don't have the key
  - But we do have code for CaesarCipher!

```
public void eyeballDecrypt(String encrypted){
   CaesarCipher cipher = new CaesarCipher();
   for(int k=0; k < 26; k++){
     String s = cipher.encrypt(encrypted,k);
     System.out.println(k+"\t"+s);
   }
}
```

What Is the Encrypted Message?

Lujyfwapvu huk zljbypaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.

```
0  Lujyfwapvu huk zljbypaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.
1  Mvkzgxbqwv ivl amkczqbg izm ncvliumvbit xizba wn bwlig'a Qvbmzvmb.
2  Nwlahycrxw jwm bnldarch jan odwmjvnwcju yjacb xo cxmjh'b Rwcnawnc.
3  Oxmbizdsyx kxn comebsdi kbo pexnkwoxdkv zkbdc yp dynki'c Sxdobxod.
4  Pyncjaetzy lyo dpnfctej lcp qfyolxpyelw alced zq ezolj'd Tyepcype.
5  Qzodkbfuaz mzp eqogdufk mdq rgzpmyqzfmx bmdfe ar fapmk'e Uzfqdzqf.
6  Rapelcgvba naq frphevgl ner shaqnzragny cnegf bs gbqnl'f Vagrearg.
7  Sbqfmdhwcb obr gsqifwhm ofs tibroasbhoz dofhg ct hcrom'g Wbhsfbsh.
8  Tcrgneixdc pcs htrjgxin pgt ujcspbtcipa epgih du idspn'h Xcitgcti.
9  Udshofjyed qdt iuskhyjo qhu vkdtqcudjqb fqhji ev jetqo'i Ydjuhduj.
10 Vetipgkzfe reu jvtlizkp riv wleurdvekrc grikj fw kfurp'j Zekvievk.
11 Wfujqhlagf sfv kwumjalq sjw xmfvsewflsd hsjlk gx lgvsq'k Aflwjfwl.
12 Xgvkrimbhg tgw lxvnkbmr tkx yngwtfxgmte itkml hy mhwtr'l Bgmxkgxm.
13 Yhwlsjncih uhx mywolcns uly zohxugyhnuf julnm iz nixus'm Chnylhyn.
14 Zixmtkodji viy nzxpmdot vmz apiyvhziovg kvmon ja ojyvt'n Diozmizo.
15 Ajynulpekj wjz oayqnepu wna bqjzwiajpwh lwnpo kb pkzwu'o Ejpanjap.
16 Bkzovmqflk xka pbzrofqv xob crkaxjbkqxi mxoqp lc qlaxv'p Fkqbokbq.
17 Clapwnrgml ylb qcaspgrw ypc dslbykclryj nyprq md rmbyw'q Glrcplcr.
18 Dmbqxoshnm zmc rdbtqhsx zqd etmczldmszk ozqsr ne snczx'r Hmsdqmds.
19 Encryption and security are fundamental parts of today's Internet.
20 Fodszqujpo boe tfdvsjuz bsf gvoebnfoubm qbsut pg upebz't Joufsofu.
21 Gpetarvkqp cpf ugewtkva ctg hwpfcogpvcn rctvu qh vqfca'u Kpvgtpgv.
22 Hqfubswlrq dqg vhfxulwb duh ixqgdphqwdo sduwv ri wrgdb'v Lqwhuqhw.
23 Irgvctxmsr erh wigyvmxc evi jyrheqirxep tevxw sj xshec'w Mrxivrix.
24 Jshwduynts fsi xjhzwnyd fwj kzsifrjsyfq ufwyx tk ytifd'x Nsyjwsjy.
25 Ktixevzout gtj ykiaxoze gxk latjgsktzgr vgxzy ul zujge'y Otzkxtkz.
```

Duke
UNIVERSITY

What Is the Encrypted Message?

Lujyfwapvu huk zljbypaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.

```
0  Lujyfwapvu huk zljbypaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.
1  Mvkzgxbqwv ivl amkczqbg izm ncvliumvbit xizba wn bwlig'a Qvbmzvmb.
2  Nwlahycrxw jwm bnldarch jan odwmjvnwcju yjacb xo cxmjh'b Rwcnawnc.
3  Oxmbizdsyx kxn comebsdi kbo pexnkwoxdkv zkbdc yp dynki'c Sxdobxod.
4  Pyncjaetzy lyo dpnfctej lcp qfyolxpyelw alced zq ezolj'd Tyepcype.
5  Qzodkbfuaz mzp eqogdufk mdq rgzpmyqzfmx bmdfe ar fapmk'e Uzfqdzqf.
6  Rapelcgvba naq frphevgl ner shaqnzragny cnegf bs gbqnl'f Vagrearg.
7  Sbqfmdhwcb obr gsqifwhm ofs tibroasbhoz dofhg ct hcrom'g Wbhsfbsh.
8  Tcrgneixdc pcs htrjgxin pgt ujcspbtcipa epgih du idspn'h Xcitgcti.
9  Udshofjyed qdt iuskhyjo qhu vkdtqcudjqb fqhji ev jetqo'i Ydjuhduj.
10 Vetipgkzfe reu jvtlizkp riv wleurdvekrc grikj fw kfurp'j Zekvievk.
11 Wfujqhlagf sfv kwumjalq sjw xmfvsewflsd hsjlk gx lgvsq'k Aflwjfwl.
12 Xgvkrimbhg tgw lxvnkbmr tkx yngwtfxgmte itkml hy mhwtr'l Bgmxkgxm.
13 Yhwlsjncih uhx mywolcns uly zohxugyhnuf julnm iz nixus'm Chnylhyn.
14 Zixmtkodji viy nzxpmdot vmz apiyvhziovg kvmon ja ojyvt'n Diozmizo.
15 Ajynulpekj wjz oayqnepu wna bqjzwiajpwh lwnpo kb pkzwu'o Ejpanjap.
16 Bkzovmqflk xka pbzrofqv xob crkaxjbkqxi mxoqp lc qlaxv'p Fkqbokbq.
17 Clapwnrgml ylb qcaspgrw ypc dslbykclryj nyprq md rmbyw'q Glrcplcr.
18 Dmbqxoshnm zmc rdbtqhsx zqd etmczldmszk ozqsr ne snczx'r Hmsdqmds.
19 Encryption and security are fundamental parts of today's Internet.
20 Fodszqujpo boe tfdvsjuz bsf gvoebnfoubm qbsut pg upebz't Joufsofu.
21 Gpetarvkqp cpf ugewtkva ctg hwpfcogpvcn rctvu qh vqfca'u Kpvgtpgv.
22 Hqfubswlrq dqg vhfxulwb duh ixqgdphqwdo sduwv ri wrgdb'v Lqwhuqhw.
23 Irgvctxmsr erh wigyvmxc evi jyrheqirxep tevxw sj xshec'w Mrxivrix.
24 Jshwduynts fsi xjhzwnyd fwj kzsifrjsyfq ufwyx tk ytifd'x Nsyjwsjy.
25 Ktixevzout gtj ykiaxoze gxk latjgsktzgr vgxzy ul zujge'y Otzkxtkz.
```

Duke UNIVERSITY

What Is the Encrypted Message?

Lujyfwapvu huk zljbypaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.

```
0  Lujyfwapvu huk zljbypaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.
1  Mvkzgxbqwv ivl amkczqbg izm ncvliumvbit xizba wn bwlig'a Qvbmzvmb.
2  Nwlahycrxw jwm bnldarch jan odwmjvnwcju yjacb xo cxmjh'b Rwcnawnc.
3  Oxmbizdsyx kxn comebsdi kbo pexnkwoxdkv zkbdc yp dynki'c Sxdobxod.
4  Pyncjaetzy lyo dpnfctej lcp qfyolxpyelw alced zq ezolj'd Tyepcype.
5  Qzodkbfuaz mzp eqogdufk mdq rgzpmyqzfmx bmdfe ar fapmk'e Uzfqdzqf.
6  Rapelcgvba naq frphevgl ner shaqnzragny cnegf bs gbqnl'f Vagrearg.
7  Sbqfmdhwcb obr gsqifwhm ofs tibroasbhoz dofhg ct hcrom'g Wbhsfbsh.
8  Tcrgneixdc pcs htrjgxin pgt ujcspbtcipa epgih du idspn'h Xcitgcti.
9  Udshofjyed qdt iuskhyjo qhu vkdtqcudjqb fqhji ev jetqo'i Ydjuhduj.
10 Vetipgkzfe reu jvtlizkp riv wleurdvekrc grikj fw kfurp'j Zekvievk.
11 Wfujqhlagf sfv kwumjalq sjw xmfvsewflsd hsjlk gx lgvsq'k Aflwjfwl.
12 Xgvkrimbhg tgw lxvnkbmr tkx yngwtfxgmte itkml hy mhwtr'l Bgmxkgxm.
13 Yhwlsjncih uhx mywolcns uly zohxugyhnuf julnm iz nixus'm Chnylhyn.
14 Zixmtkodji viy nzxpmdot vmz apiyvhziovg kvmon ja ojyvt'n Diozmizo.
15 Ajynulpekj wjz oayqnepu wna bqjzwiajpwh lwnpo kb pkzwu'o Ejpanjap.
16 Bkzovmqflk xka pbzrofqv xob crkaxjbkqxi mxoqp lc qlaxv'p Fkqbokbq.
17 Clapwnrgml ylb qcaspgrw ypc dslbykclryj nyprq md rmbyw'q Glrcplcr.
18 Dmbqxoshnm zmc rdbtqhsx zqd etmczldmszk ozqsr ne snczx'r Hmsdqmds.
19 Encryption and security are fundamental parts of today's Internet.
20 Fodszqujpo boe tfdvsjuz bsf gvoebnfoubm qbsut pg upebz't Joufsofu.
21 Gpetarvkqp cpf ugewtkva ctg hwpfcogpvcn rctvu qh vqfca'u Kpvgtpgv.
22 Hqfubswlrq dqg vhfxulwb duh ixqgdphqwdo sduwv ri wrgdb'v Lqwhuqhw.
23 Irgvctxmsr erh wigyvmxc evi jyrheqirxep tevxw sj xshec'w Mrxivrix.
24 Jshwduynts fsi xjhzwnyd fwj kzsifrjsyfq ufwyx tk ytifd'x Nsyjwsjy.
25 Ktixevzout gtj ykiaxoze gxk latjgsktzgr vgxzy ul zujge'y Otzkxtkz.
```

Duke UNIVERSITY

What Is the Encrypted Message?

Lujyfwapvu huk zljbypaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.

```
0  Lujyfwapvu huk zljbypaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.
1  Mvkzgxbqwv ivl amkczqbg izm ncvliumvbit xizba wn bwlig'a Qvbmzvmb.
2  Nwlahycrxw jwm bnldarch jan odwmjvnwcju yjacb xo cxmjh'b Rwcnawnc.
3  Oxmbizdsyx kxn comebsdi kbo pexnkwoxdkv zkbdc yp dynki'c Sxdobxod.
4  Pyncjaetzy lyo dpnfctej lcp qfyolxpyelw alced zq ezolj'd Tyepcype.
5  Qzodkbfuaz mzp eqogdufk mdq rgzpmyqzfmx bmdfe ar fapmk'e Uzfqdzqf.
6  Rapelcgvba naq frphevgl ner shaqnzragny cnegf bs gbqnl'f Vagrearg.
7  Sbqfmdhwcb obr gsqifwhm ofs tibroasbhoz dofhg ct hcrom'g Wbhsfbsh.
8  Tcrgneixdc pcs htrjgxin pgt ujcspbtcipa epgih du idspn'h Xcitgcti.
9  Udshofjyed qdt iuskhyjo qhu vkdtqcudjqb fqhji ev jetqo'i Ydjuhduj.
10 Vetipgkzfe reu jvtlizkp riv wleurdvekrc grikj fw kfurp'j Zekvievk.
11 Wfujqhlagf sfv kwumjalq sjw xmfvsewflsd hsjlk gx lgvsq'k Aflwjfwl.
12 Xgvkrimbhg tgw lxvnkbmr tkx yngwtfxgmte itkml hy mhwtr'l Bgmxkgxm.
13 Yhwlsjncih uhx mywolcns uly zohxugyhnuf julnm iz nixus'm Chnylhyn.
14 Zixmtkodji viy nzxpmdot vmz apiyvhziovg kvmon ja ojyvt'n Diozmizo.
15 Ajynulpekj wjz oayqnepu wna bqjzwiajpwh lwnpo kb pkzwu'o Ejpanjap.
16 Bkzovmqflk xka pbzrofqv xob crkaxjbkqxi mxoqp lc qlaxv'p Fkqbokbq.
17 Clapwnrgml ylb qcaspgrw ypc dslbykclryj nyprq md rmbyw'q Glrcplcr.
18 Dmbqxoshnm zmc rdbtqhsx zqd etmczldmszk ozqsr ne snczx'r Hmsdqmds.
19 Encryption and security are fundamental parts of today's Internet.
20 Fodszqujpo boe tfdvsjuz bsf gvoebnfoubm qbsut pg upebz't Joufsofu.
21 Gpetarvkqp cpf ugewtkva ctg hwpfcogpvcn rctvu qh vqfca'u Kpvgtpgv.
22 Hqfubswlrq dqg vhfxulwb duh ixqgdphqwdo sduwv ri wrgdb'v Lqwhuqhw.
23 Irgvctxmsr erh wigyvmxc evi jyrheqirxep tevxw sj xshec'w Mrxivrix.
24 Jshwduynts fsi xjhzwnyd fwj kzsifrjsyfq ufwyx tk ytifd'x Nsyjwsjy.
25 Ktixevzout gtj ykiaxoze gxk latjgsktzgr vgxzy ul zujge'y Otzkxtkz.
```

Duke UNIVERSITY