

# Breaking the Caesar Cipher

## Introduction

# 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 zljbyfaf 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?

***Lujoyfwapvu huk zljbyfaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.***

0 Lujoyfwapvu huk zljbyfaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.  
1 Mvkzgbqvw 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 rgzpmqzfm x bmdfe ar fapmk'e Uzfqdzqf.  
6 Rapelcgvba naq frphevgl ner shaqnzrag ny cnegf bs gbqnl'f Vagrearg.  
7 Sbaqmdhwcb obr gsqifwhm ofs tibroasbhoz dof hg ct hcrom'g Wbhsfbsh.  
8 Tcrgneixdc pcs htrjgxin pgt ujcsbptcipa epgih du idspn'h Xcitgcti.  
9 Udshofjyed qdt iuskhyjo qhu vkdtqcudjqb fqhji ev jetqo'i Ydjuhduj.  
10 Vetipgkzfe reu jvtlizkp riv wleurdvekrc gri kj fw kfurp'j Zekvievk.  
11 Wfujqhlagf sfv kwumjalq sjw xmfvsewflsd hsjlk gx lgvsq'k Aflwjfwl.  
12 Xgvkrimbhg tgw lxvnbkmr tkx yngwtfxgmte itkml hy mhwtr'l Bgm xkgxm.  
13 Yhwlsjncih uhx mywolcns uly zohxugyhnuf julnm iz nixus'm Chnylhyn.  
14 Zixmtkodji viy nzxpm dot vmz apiyvhziovg kvmon ja ojyvt'n Diozmizo.  
15 Ajynulpekj wjz oayqnepu wna bqjzwiajpwh lwnpo kb pkz wu'o Ejpanjap.  
16 Bkzovmqflk xka pbzrofqv xob crkaxjbkqxi mxoqp lc qlaxv'p Fkqbokbq.  
17 Clapwnrgml ylb qcaspg rw 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 vhf xulwb duh ixqgdphqwdo sduwv ri wr gdb'v Lqwhuqhw.  
23 Irgvctxmsr erh wigyvmxc evi jyrheqirxep tevw sj xshec'w Mrxivrix.  
24 Jshwduynts fsi xjhzwnyd fwj kzsifrjsyfq ufwyx tk ytifd'x Nsyjwsjy.  
25 Ktixevzout gtj ykioxoze gxk latjgsktzgr vgxzy ul zujge'y Otkxtkz.





# What Is the Encrypted Message?

***Lujoyfwapvu huk zljbyfaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.***

0 Lujoyfwapvu huk zljbyfaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.  
1 Mvkzgbqvw ivl amkczqbg izm ncvliumvbit xizba wn bwlig'a Qvbmzvmb.  
2 Nwlahycrxw jwm bnldarch jan odwmjvnwcju yjacb xo cxmjh'b Rwcnawnc.  
3 Oxmbizdsyx knx comebsdi kbo pexnkwoxdkv zkbdc yp dynki'c Sxdobxod.  
4 Pyncjaetzy lyo dpnfctej lcp qfyolxpyelw alced zq ezolj'd Tyepcype.  
5 Qzodkbfuaz mzp eqogdufk mdq rgzpmqzfm x bmdfe ar fapmk'e Uzfqdzqf.  
6 Rapelcgvba naq frphevgl ner shaqnzragny cnegf bs gbqnl'f Vagrearg.  
7 Sbaqmdhwcb obr gsqifwhm ofs tibroasbhoz dofhg ct hcrom'g Wbhsfbsh.  
8 Tcrgneixdc pcs htrjgxin pgt ujcsbptcipa 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 lxvnbkmr tkx yngwtfxgmte itkml hy mhwtr'l Bgmxxgxm.  
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 qcaspgwr 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 vhfuxlwb duh ixqgdphqwdo sduwv ri wrqdb'v Lqwhuqhw.  
23 Irgvctxmsr erh wigvymxc evi jyrheqirxep tevwx 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 Otkxxtkz.





# What Is the Encrypted Message?

***Lujoyfwapvu huk zljbyfaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.***

0 Lujoyfwapvu huk zljbyfaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.  
1 Mvkzgbqvw 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 rgzpmqzfm x bmdfe ar fapmk'e Uzfqdzqf.  
6 Rapelcgvba naq frphevgl ner shaqnzragny cnegf bs gbqnl'f Vagrearg.  
7 Sbaqmdhwcb obr gsqifwhm ofs tibroasbhoz dofhg ct hcrom'g Wbhsfbsh.  
8 Tcragneixdc pcs htrjgxin pgt ujcsbptcipa 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 lxvnbkmr tkx yngwtfxgmte itkml hy mhwtr'l Bgm xkgxm.  
13 Yhwlsjncih uhx mywolcns uly zohxugyhnuf julnm iz nixus'm Chnylhyn.  
14 Zixmtkodji viy nzxpm dot vmz apiyvhziovg kvmon ja ojyvt'n Diozmizo.  
15 Ajynulpekj wjz oayqnepu wna bajzwiajpwh 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 Dmbaxoshnm 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 vhf xulwb duh ixqgdphqwd sduwv ri wrgdb'v Lqwhuqhw.  
23 Irgvctxmsr erh wigyv mxc evi jyrheqirxep tevwx 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 Otkxtkz.





# What Is the Encrypted Message?

***Lujoyfwapvu huk zljbyfaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.***

0 Lujoyfwapvu huk zljbyfaf hyl mbukhtluahs whyaz vm avkhf'z Pualyula.  
1 Mvkzgbqvw ivl amkczqbg izm ncvliumvbit xizba wn bwlig'a Qvbmzvmb.  
2 Nwlahycrxw jwm bnldarch jan odwmjvnwcju yjacb xo cxmjh'b Rwcnawnc.  
3 Oxmbizdsyx knx comebsdi kbo pexnkwoxdkv zkbdc yp dynki'c Sxdobxod.  
4 Pyncjaetzy lyo dpnfctej lcp qfyolxpyelw alced zq ezolj'd Tyepcype.  
5 Qzodkbfuaz mzp eqogdufk mdq rgzpmqzfm x bmdfe ar fapmk'e Uzfqdzqf.  
6 Rapelcgvba naq frphevgl ner shaqnzragny cnegf bs gbqnl'f Vagrearg.  
7 Sbaqmdhwcb obr gsqifwhm ofs tibroasbhoz dofhg ct hcrom'g Wbhsfbsh.  
8 Tcragneixdc pcs htrjgxin pgt ujcsbptcipa 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 lxvnbkmr tkx yngwtfxgnte itkml hy mhwtr'l Bgm xkgxm.  
13 Yhwlsjncih uhx mywolcns uly zohxugyhnuf julnm iz nixus'm Chnylhyn.  
14 Zixmtkodji viy nzxpm dot vmz apiyvhziovg kvmon ja ojyvt'n Diozmizo.  
15 Ajynulpekj wjz oayqnepu wna bajzwiajpwh lwnpo kb pkz wu'o Ejpanjap.  
16 Bkzovmqflk xka pbzrofqv xob crkaxjbkqxi mxoqp lc qlaxv'p Fkqbokbq.  
17 Clapwnrgml ylb qcaspgwr 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 vhf xulwb duh ixqgdphqwdo sduwv ri wrgdb'v Lqwhuqhw.  
23 Irgvctxmsr erh wigyv mxc evi jyrheqirxep tevwx 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 Otkxtkz.

