An toàn Bảo mật thông tin (Mật mã cổ điển)

Giáo viên: Phạm Nguyên Khang
pnkhang@cit.ctu.edu.vn

Nội dung

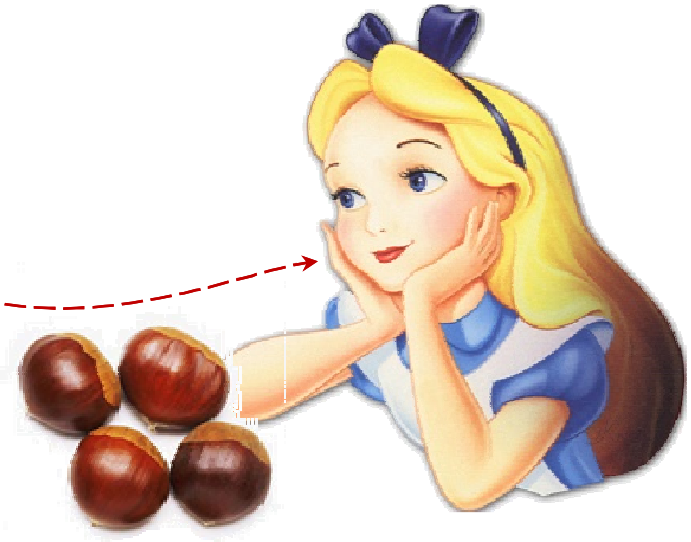
- Tổng quan về an toàn và bảo mật thông tin
- Các hệ mật mã cổ điển
  - Mật mã thay thế
    - Mật mã Ceasar
    - Mật mã Playfair
    - Mật mã Hill
    - Mật mã Vigenere
  - Mật mã hoán vị
    - Mật mã rail-fence
    - Kỹ thuật hoán vị nâng cao

Tổng quan

Mình đã biết hết những gì bọn chúng trao đổi với nhau.

Bí mật

Tổng quan



Toàn vẹn

Tổng quan

- Tôi là nhà quản trị
- Cho người dùng **A** được phép đọc file M

- Tôi là nhà quản trị
- Cho phép người dùng H được phép đọc file M

Chứng thực

Tổng quan

Mua cho tôi
1000 cổ phiếu
của công ty ABC

Không từ chối trách nhiệm

Tôi đâu có nhờ
anh mua cổ
phiếu cho tôi.

Cô chuyển tiền
cho tôi đi chứ !

Tổng quan

- Các hành vi xâm phạm
  - Xâm phạm thụ động: liên quan đến việc nghe lén hoặc quan sát thông tin được truyền đi
    - Tách nội dung thông điệp: thu các thông tin nhạy cảm trong thư điện tử hay trong các tập tin truyền đi.
    - Phân tích đường truyền: thông tin nhạy cảm có thể được che dấu bằng mã hóa, nhưng đối thủ có thể xác định vị trí các thực thể và quan sát tần suất và độ dài của thông điệp để rút trích bản chất của thông điệp.

  → Xâm phạm thụ động khó phát hiện vì không có ảnh hưởng đến tài nguyên và thao tác của hệ thống → tập trung phòng chống.

Tổng quan

- Các hành vi xâm phạm
  - Xâm phạm chủ động: liên quan đến việc thay đổi dữ liệu hoặc tạo dữ liệu sai
    - Giả mạo: thực hiện các thao tác theo sau một chứng thực hợp lệ để sử dụng các quyền của người dùng hợp lệ cho các thao tác "không hợp lệ" trong hệ thống.
    - Làm lại (replay): truyền lại các gói tin của lần chứng thực hợp lệ của quá khứ cho các lần chứng thực trong tương lai.
    - Thay đổi thông điệp: một phần hoặc toàn bộ thông tin hợp pháp bị thay thế bằng các thông tin giả mạo nhằm thực hiện các tác vụ không cho phép.
    - Từ chối dịch vụ (denial of service): ngăn chặn hay gây ức chế việc sử dụng và quản lý thông thường của các thiết bị truyền thông.

  → Dễ phát hiện nhưng khó ngăn chặn

Tổng quan

- Các biện pháp bảo vệ thông tin
  - Hành chính
  - Thiết bị kỹ thuật (phần cứng)
  - Thuật toán (phần mềm)
- Nhận xét
  - Hiệu quả và kinh tế nhất: thuật toán
  - Thực tế: kết hợp cả 3 biện pháp

Một số thuật ngữ

- Bản rõ (**P**laintext): thông báo gốc cần chuyển, được ghi bằng hình ảnh, âm thanh, chữ số, chữ viết…
- Bản mật/Bản mã (**C**iphertext): "ngụy trang" bản rõ thành một dạng khác để người "ngoài cuộc" không thể đọc được
- Mật mã hóa/lập mã (**E**ncryption): quá trình biến đổi bản rõ thành bản mật
- Giải mật mã/giải mã (**D**ecryption): quá trình biến đổi bản mật thành bản rõ
- Hệ mã (Cryptosystem): một phương pháp ngụy trang bản rõ. Nghệ thuật tạo ra và sử dụng các hệ mật mã được gọi là thuật mật mã hóa hay mật mã học (**Cryptography**)
- Phân tích mã/thám mã (Cryptanalysis): nghệ thuật phá các hệ mật mã

Giải thuật mật mã hóa

- Các hệ mật mã hóa được mô tả bằng 3 đặc tính
  - Kiểu của các thao tác được dùng để biến đổi bản rõ thành bản mật: tất cả các giải thuật mã hóa đều dựa trên 2 nguyên lý
    - Thay thế (substitution): mỗi thành phần trong bản rõ (bit, ký tự, nhóm các bit hay các ký tự) được ánh xạ đến thành phần khác.
    - Chuyển vị (transposition): các thành phần trong bản rõ được sắp xếp lại.

    Yêu cầu cơ bản: thông tin không bị mất (các thao tác đều khả đảo)

    Phần lớn các hệ mã kết hợp cả 2 nguyên lý qua nhiều bước.
  - Số khóa được sử dụng:
    - 1 Khóa: người gởi và người nhận sử dụng chung khóa?
    - 2 Khóa: Khóa bí mật/Khóa công khai
      - Mật hóa dùng 1 khóa và giải mật mã dùng 1 khóa khác

Giải thuật mật mã hóa (tt)

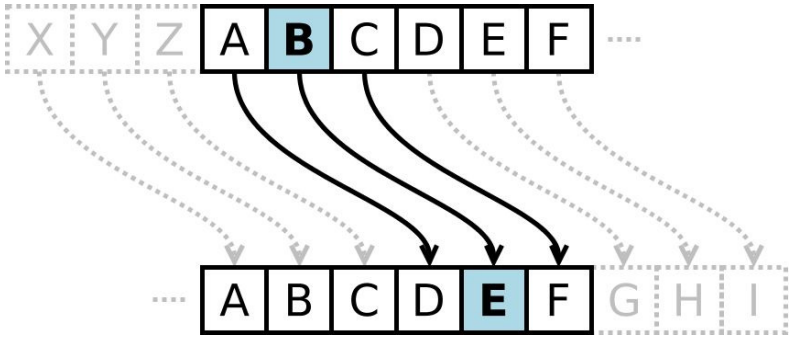
- Cách thức bản rõ được xử lý:
  - Mã hóa khối (block cipher) xử lý từng khối dữ liệu tại một thời điểm, sản sinh một khối dữ liệu ở đầu ra.
  - Mã hóa luồng (stream cipher) xử lý các phần tử liên tục và sản sinh từng phần tử một ở đầu ra tại một thời điểm.

Các hệ mật mã cổ điển

- Kỹ thuật thay thế
  - Mật mã Ceasar
  - Mật mã Playfair
  - Mật mã Hill
- Kỹ thuật hoán vị
  - Mật mã rail fence
  - Kỹ thuật hoán vị nâng cao

Mật mã Ceasar

- Mật mã Ceasar:
  - Mật mã đơn ký tự
  - Thay thế mỗi ký tự bằng một ký tự khác cách nhau một khoảng cách nhất định trong bảng chữ cái.



- Biểu diễn toán học

$$C = E(p) = (p + k) \bmod 26$$

$$p = D(C) = (C - k) \bmod 26$$

k: khóa của giải thuật

Mật mã Ceasar

- Áp dụng mật mã Ceasar mật mã hóa các bản rõ sau với khóa k = 4
  - **actions speak louder than words**

- Đoán khóa **k** và giải mật cho bản mật sau:
  - **ST RFS HFS XJWAJ YBT RFXYJWX**

Mật mã Ceasar

- Có thể bị tấn công theo kiểu vét cạn (brute-force) bằng cách thử hết tất cả 25 khóa

	TIPGKFXIRGYPZEYZJKFIPZJZEKVIVJKZEX		TIPGKFXIRGYPZEYZJKFIPZJZEKVIVJKZEX
1	UJQHLGYJSHZQAFZAKLGJQAKAFLWJWKLAFY	14	HWDUYTLWFUMDNSMNXYTWDNXNSYJWJXYNSL
2	VKRIMHZKTIARBGABLMHKRBLBGMXKXLMBGZ	15	IXEVZUMXGVNEOTNOYZUXEOYOTZKXKYZOTM
3	WLSJNIALUJBSCHBCMNILSCMCHNYLYMNCHA	16	JYFWAVNYHWOFPUOPZAVYFPZPUALYLZAPUN
4	XMTKOJBMVKCTDICDNOJMTDNDIOZMZNODIB	17	KZGXBWOZIXPGQVPQABWZGQAQVBMZMABQVO
5	YNULPKCNWLDUEJDEOPKNUEOEJPANAOPEJC	18	LAHYCXPAJYQHRWQRBCXAHRBRWCNANBCRWP
6	ZOVMQLDOXMEVFKEFPQLOVFPFKQBOBPQFKD	19	MBIZDYQBKZRISXRSCDYBISCSXDOBOCDSXQ
7	APWNRMEPYNFWGLFGQRMPWGQGLRCPCQRGLE	20	NCJAEZRCLASJTYSTDEZCJTDTYEPCPDETYR
8	BQXOSNFQZOGXHMGHRSNQXHRHMSDQDRSHMF	21	ODKBFASDMBTKUZTUEFADKUEUZFQDQEFUZS
9	CRYPTOGRAPHYINHISTORYISINTERESTING	22	PELCGBTENCULVAUVFGBELVFVAGRERFGVAT
10	DSZQUPHSBQIZJOIJTUPSZJTJOUFSFTUJOH	23	QFMDHCUFODVMWBVWGHCFMWGWBHSFSGHWBU
11	ETARVQITCRJAKPJKUVQTAKUKPVGTGUVKPI	24	RGNEIDVGPEWNXCWXHIDGNXHXCITGTHIXCV
12	FUBSWRJUDSKBLQKLVWRUBLVLQWHUHVWLQJ	25	SHOFJEWHQFXOYDXYIJEHOYIYDJUHUIJYDW
13	GVCTXSKVETLCMRLMWXSVCMWMRXIVIWXMRK		

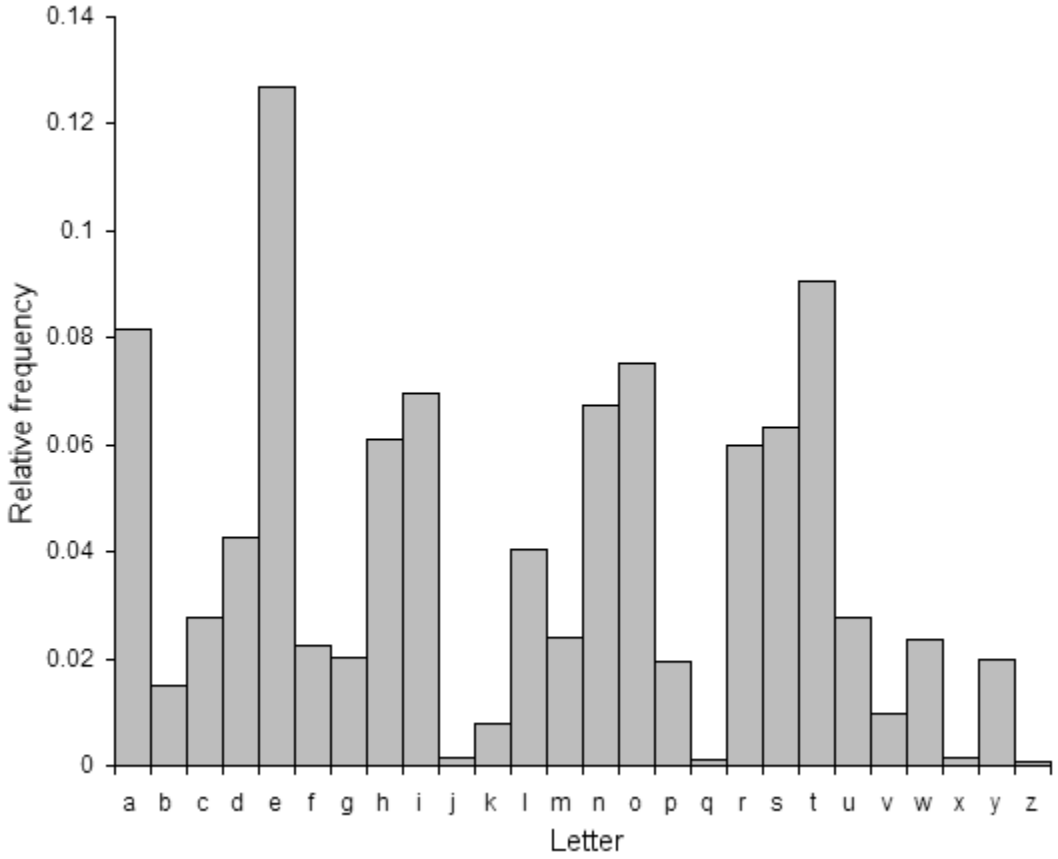
Mật mã Ceasar

- Nhận xét: 3 đặc điểm chính để áp dụng tấn công theo kiểu brute-force trong thuật toán này
  - Giải thuật mã hóa và giải mã được biết trước
  - Số khóa để thử rất ít
  - Ngôn ngữ của bản rõ được biết trước và dễ dàng nhận ra
- Giải quyết vấn đề (tổng quát)
  - Sử dụng nhiều khóa
  - bản rõ có thể được nén lại (Huffman, ZIP) để cho người đọc khó nhận ra ngôn ngữ sử dụng

Mật mã đơn ký tự

- Sử dụng hoán vị 26 chữ cái → có $26!=4.10^{26}$ khóa.
- Nhận xét: tần số xuất hiện của các chữ cái trong các ngôn ngữ là cố định

Mật mã đơn ký tự



Mật mã Playfair

- Mật mã đa ký tự (mỗi lần mã 2 ký tự liên tiếp nhau)
- Giải thuật dựa trên một ma trận các chữ cái 5×5 được xây dựng từ một khóa (chuỗi các ký tự)

1. Xây dựng ma trận khóa
   - Lần lượt thêm từng ký tự của khóa vào ma trận
   - Nếu ma trận chưa đầy, thêm các ký tự còn lại trong bảng chữ cái vào ma trận theo thứ tự A - Z
   - I và J la xem như 1 ký tự
   - Các ký tự trong ma trận không được trùng nhau
2. Mật mã hóa
3. Giải mật mã

Mật mã Playfair

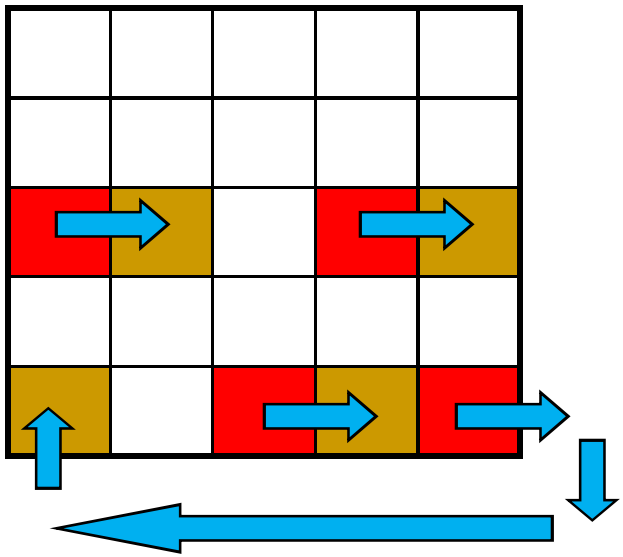
- Ví dụ: với từ khóa "playfair example"
  - Ma trận khóa

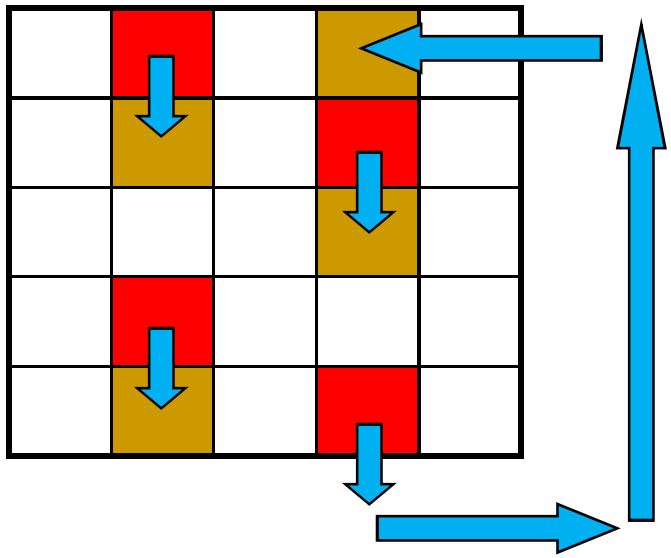
```
P L A Y F
I R E X M
B C D G H
K N O Q S
T U V W Z
```

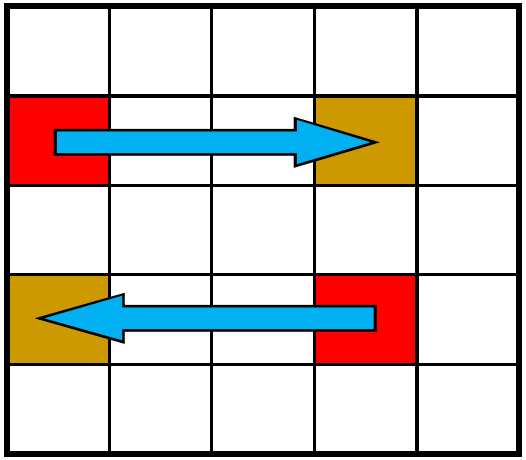
Mật mã Playfair

- Giải thuật mật mã hóa
  - Mã hóa từng cặp "2 ký tự" liên tiếp nhau.
  - Nếu 2 ký tự này giống nhau thì thêm một ký tự 'x' vào giữa.
  - VD: balloon tách thành ba lx lo on (vì ll ➔ lx l)
  - Nếu dư 1 ký tự thì thêm vào ký tự 'q' vào cuối.
  - VD: hat ➔ ha tq
  - Nếu 2 ký tự nằm cùng dòng được thay thế bằng 2 ký tự tương ứng **bên phải**. Ký tự ở cột cuối cùng được thay bằng ký tự ở cột đầu tiên.
  - Nếu 2 ký tự nằm cùng cột được thay thế bằng 2 ký tự **bên dưới**. Ký tự ở hàng cuối cùng được thay thế bằng ký tự ở hàng trên cùng
  - Nếu 2 ký tự lập thành hình chữ nhật được thay thế bằng 2 ký tự tương ứng trên cùng dòng ở hai góc còn lại.

Mật mã Playfair







Mật mã Playfair

- Ví dụ:
- Mật mã hóa bản rõ sau:
  - **hide the gold in the tree stump**

- Xem lời giải

Mật mã Hill

- Giải thuật sử dụng m ký tự liên tiếp của bản rõ và thay thế m ký tự khác trong bản mật.
- Việc thay thế được thực hiện bởi một phương trình tuyến tính trên các ký tự được gán trị (a=0, b=1, c=2…), m=3:

$$\begin{pmatrix} c1 \\ c2 \\ c3 \end{pmatrix} = \begin{pmatrix} k11 & k12 & k13 \\ k21 & k22 & k23 \\ k31 & k32 & k33 \end{pmatrix} \begin{pmatrix} p1 \\ p2 \\ p3 \end{pmatrix} \bmod 26$$

$$C = KP \mod 26$$

- Giải mã:

$$P = K^{-1}C \mod 26$$

Mật mã Hill

- Mật mã hóa bản rõ sau:
  - **pay more money**

- Với ma trận khóa:

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Mật mã Hill

- Tìm ma trận nghịch đảo của ma trận khóa K
  - Sử dụng phương pháp tìm ma trận nghịch đảo của đại số tuyến tính
  - Viết ma trận khóa K và ma trận đơn vị I cạnh nhau

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

  - Áp dụng các phép biến đổi tuyến tính lên cả hai ma trận K và I để biến K thành I. Khi đó I sẽ thành K^{-1}.
- **Chú ý:** các phép biến toán thực hiện trên vành modulo 26.

Mật mã Vigenère

- Khóa: dãy m số nguyên:
  - K = (K[0], K[1], …, K[m-1])

- Mật hóa:
  - Mật hóa từng ký tự của bản rõ
  - Ký tự thứ i của bản rõ (p[i]) được mã hóa thành

  C[i] = (p[i] + k[i mod m]) mod 26

- Giải mật:
  - Thảo luận

Mật mã Vigenère

- Ví dụ:
  - Từ khóa "Lemon"
  - Bản rõ:
    - ATTACKATDAWN
  - Bản mật:
    - Xem lời giải

Mật mã Vigenère

- Mật mã Vigenère bằng phương pháp tra bảng
  - Ghép khóa cho chiều dài khóa bằng chiều dài của bảng rõ:
  - Ví dụ với từ khóa "Lemon"
  - Bản rõ: ATTACKATDAWN
  - ➔Khóa : LEMONLEMONLE

Mật mã Vigenère

- Mật mã hóa/giải mật mã:
  - bản rõ ⇔ cột
  - khóa ⇔ hàng
  - bản mật ⇔ giao điểm.

Mật mã Vigenère

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

Mật mã rail fence

- Tách bản rõ thành hai hàng
- Ví dụ: bản rõ "meet me at the toga party" được viết thành

  m e m a t e o a a t

  e t e t h t g p r y

  bản mật: memateoaatetethtgpry

Các kỹ thuật hoán vị - nâng cao

- bản rõ được viết trên một hình chữ nhật và đọc theo cột. Thứ tự các cột trở thành khóa của giải thuật.
- Ví dụ

Key	4 1 2 5 3 6
bản rõ	m e e t m e
	a t t h e t
	o g a p a r
	t y x y z w
bản mật	**etgyetaxmeazmaotthpyetrw**

- Để tăng độ mật, có thể áp dụng hoán vị nhiều lần

Các kỹ thuật thay thế - Playfair

- Ví dụ: mật mã playfair
  - Bản rõ:

    hide the gold in the tree stump

  - Bản mật:

    BM OD ZB XD NA BE KU DM UI XM MO UV IF

Mật mã Vigenère

- Ví dụ với từ khóa "Lemon"
- Bản rõ:
  - ATTACKATDAWN
- Bản mật:
  - Xem lời giải
- Key: LEMONLEMONLE Plaintext: Ciphertext:LXFOPVEFRNHR
- Nhận xét:
- Khóa có chiều dài bằng với bản rõ.
- Mã hóa, giải mã: bản rõ theo cột, khóa theo hàng, bản mật là giao điểm.