Week 3: Autokey ciphers, cribs, and block ciphers

Jay Daigle

Occidental College

September 14, 2017

Definition

A crib is a known or guessed portion of the plaintext, which can be used to help cryptanalyze a ciphertext.

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
```

OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD IRF SNI JAM GPW

Let's guess the word "the" is in the message somewhere.

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

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

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

Let's assume the "aso" was real and see what we can conclude.

Key Length of Four

Key Length of Four

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
--- --- --- --- --- --f bn- the -as o-- --- --- --- --- ---
--- --- --- ---
--- --- --- --- --- --t he- aso -gu s-- --- --- --- --- ---
--- --- --- ---
```

Key Length of Four

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
--- --- --- --- --- --f bn- the -as o-- --- --- --- --- ---
--- --- --- ---
--- --- --- --- --- --t he- aso -gu s-- --- --- --- --- ---
--- --- --- ---
```

“fbn” isn’t very likely.

Key Length of Five

Key Length of Five

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
--- --- --- --- --- -er e-- the --a so- --- --- --- --- ---
--- --- --- ---
--- --- --- --- --- -th e-- aso --m ob- --- --- --- --- ---
--- --- --- ---
```

Key Length of Five

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
--- --- --- --- --- -er e-- the --a so- --- --- --- --- ---
--- --- --- ---
--- --- --- --- --- -th e-- aso --m ob- --- --- --- --- ---
--- --- --- ---
```

This looks better...

Key Length of Five

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
--- --- ono --m di- -er e-- the --a so- -mo b-- auo --- ---
--- --- --- ---
--- --- mdi --e re- -th e-- aso --m ob- -au o-- ncj --- ---
--- --- --- ---
```

This looks better...but this doesn't.

Key Length of Six

Key Length of Six

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
--- --- --- --- --- gqu --- the --- aso --- --- --- --- ---
--- --- --- ---
--- --- --- --- --- the --- aso --- gxw --- --- --- --- ---
--- --- --- ---
```

Key Length of Six

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
--- --- --- --- --- gqu --- the --- aso --- --- --- --- ---
--- --- --- ---
--- --- --- --- --- the --- aso --- gxw --- --- --- --- ---
--- --- --- ---
```

“gxw” and “gqu” both look bad.

Key Length of Six

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
--- --- --- --- --- gqu --- the --- aso --- --- --- --- ---
--- --- --- ---
--- --- --- --- --- the --- aso --- gxw --- --- --- --- ---
--- --- --- ---
```

“gxw” and “gqu” both look bad.

We could keep trying longer keywords. We won’t get anywhere.

A new offset?

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

A new offset?

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

Key Length of Four

Key Length of Four

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
--- --- --- -wj q-t he- est --- --- --- --- --- --- --- ---
--- --- --- ---
--- --- --- -th e-e st- ezr --- --- --- --- --- --- --- ---
--- --- --- ---
```

Key Length of Four

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
--- --- --- -wj q-t he- est --- --- --- --- --- --- --- ---
--- --- --- ---
--- --- --- -th e-e st- ezr --- --- --- --- --- --- --- ---
--- --- --- ---
```

Nope.

Key Length of Five

Key Length of Five

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
--- --- --- tim --t he- -es t-- --- --- --- --- --- --- ---
--- --- --- ---
--- --- --- the --e st- -ns a-- --- --- --- --- --- --- ---
--- --- --- ---
```

Key Length of Five

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
--- --- --- tim --t he- -es t-- --- --- --- --- --- --- ---
--- --- --- ---
--- --- --- the --e st- -ns a-- --- --- --- --- --- --- ---
--- --- --- ---
```

Promising....

Key Length of Five

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
--- --s o-- tim --t he- -es t-- nsa --- --- --- --- --- ---
--- --- --- ---
so- --i m-- the --e st- -ns a-- com --- --- --- --- --- ---
--- --- --- ---
```

Promising....

Key Length of Five

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
wa- --s o-- tim --t he- -es t-- nsa --c om- -ic a-- dan --h
ea- -we r-- res
so- --i m-- the --e st- -ns a-- com --i ca- -da n-- hea --w
er- -re s-- ple
```

Promising....And now it's a fill-in-the-blank puzzle.

Key Length of Five

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
wa- --s o-- tim --t he- -es t-- nsa --c om- -ic a-- dan --h
ea- -we r-- res
so- --i m-- the --e st- -ns a-- com --i ca- -da n-- hea --w
er- -re s-- ple
```

Promising....And now it's a fill-in-the-blank puzzle.

Key Length of Five

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
wa- --s o-- tim --t he- -es t-- nsa --c om- -ic a-- dan --h
ea- -we r-- res
so- --i m-- the --e st- -ns a-- com --i ca- -da n-- hea --w
er- -re sim ple
```

Promising....And now it's a fill-in-the-blank puzzle.

Key Length of Five

```
OOF IKA AQW MPQ UMX ZXY IRK TZS PGM GPK QMI PLC NWX KEN QLD
IRF SNI JAM GPW
wat ers ome tim est heq ues tio nsa rec omp lic ate dan dth
ean swe rsa res
som eti mes the que sti ons are com pli cat eda ndt hea nsw
ers are sim ple
```

Done!

"Sometimes the questions are complicated, and the answers are simple."
Theodor Geisel

"Sometimes the questions are complicated, and the answers are simple."
Theodor Geisel a.k.a. Dr. Seuss

Definition

A block cipher encrypts fixed-sized blocks of ciphertext, rather than single letters at a time.

Permutation cipher

We choose a block size n, and as a key choose an element $k \in S_n$, which is a permutation on an alphabet of n letters.

Permutation cipher

We choose a block size n, and as a key choose an element $k \in S_n$, which is a permutation on an alphabet of n letters.
To encrypt, we break our plaintext into blocks of size n, padding the final block with nonsense characters if necessary. Then we permute each block according to the key k.

Permutation cipher

We choose a block size n, and as a key choose an element $k \in S_n$, which is a permutation on an alphabet of n letters.
To encrypt, we break our plaintext into blocks of size n, padding the final block with nonsense characters if necessary. Then we permute each block according to the key k.
To decrypt, we take the inverse permutation k^{-1} and apply this to each ciphertext block.

"Fourscore and seven years ago"

"Fourscore and seven years ago"

Block size five

"Fourscore and seven years ago"

Block size five and key $k = (12345) \mapsto (23514)$.

"Fourscore and seven years ago"

Block size five and key $k = (12345) \mapsto (23514)$.

`fours corea ndsev enyea rsago`

"Fourscore and seven years ago"

Block size five and key $k = (12345) \mapsto (23514)$.

`fours corea ndsev enyea rsago`

`RFOSU`

“Fourscore and seven years ago”

Block size five and key $k = (12345) \mapsto (23514)$.

`fours corea ndsev enyea rsago`

`RFOSU`

"Fourscore and seven years ago"

Block size five and key $k = (12345) \mapsto (23514)$.

`fours corea ndsev enyea rsago`

`RFOSU`

"Fourscore and seven years ago"

Block size five and key $k = (12345) \mapsto (23514)$.

`fours corea ndsev enyea rsago`

`RFOSU`

"Fourscore and seven years ago"

Block size five and key $k = (12345) \mapsto (23514)$.

`fours corea ndsev enyea rsago`

`RFOSU`

“Fourscore and seven years ago”

Block size five and key $k = (12345) \mapsto (23514)$.

`fours corea ndsev enyea rsago`

`RFOSU`

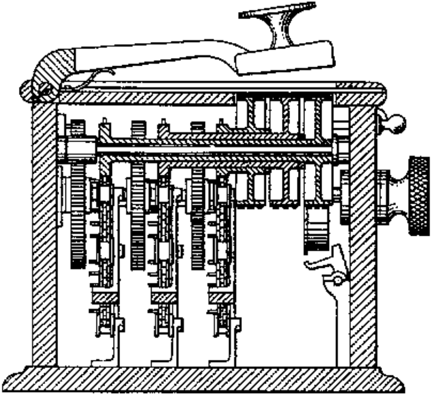
“Fourscore and seven years ago”

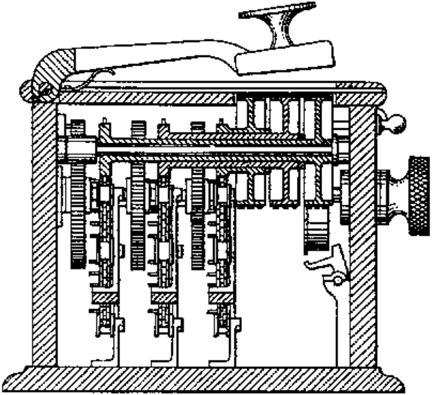
Block size five and key $k = (12345) \mapsto (23514)$.

`fours corea ndsev enyea rsago`

`RFOSU ECOAR ENDVS EENAY GRSOA.`

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \left(\det \begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$





Lester Hill's patented cipher machine

Hill Cipher

We first choose a block size n. We choose a key, which is a $n \times n$ matrix K with entries in $\mathbb{Z}/26\mathbb{Z}$ (that is, integers modulo 26). We require that $\gcd(26, \det K) = 1$.

We divide our message into blocks of length n. We write each plaintext block as a column vector $B \in (\mathbb{Z}/26\mathbb{Z})^n$. The corresponding ciphertext block is given by KB.

To decrypt, we compute K^{-1} in $\mathbb{Z}/26\mathbb{Z}$. Given a ciphertext block C, the corresponding plaintext block is $K^{-1}C$.

"It was a dark and stormy night."

"It was a dark and stormy night."

```
IT WA SA DA RK AN DS TO RM YN IG HT
```

"It was a dark and stormy night."

`IT WA SA DA RK AN DS TO RM YN IG HT`

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

“It was a dark and stormy night.”

`IT WA SA DA RK AN DS TO RM YN IG HT`

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$K \begin{bmatrix} 8 \\ 19 \end{bmatrix} = \begin{bmatrix} 43 \\ 78 \end{bmatrix} \equiv \begin{bmatrix} 17 \\ 0 \end{bmatrix}$$

"It was a dark and stormy night."

`IT WA SA DA RK AN DS TO RM YN IG HT`

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$K \begin{bmatrix} 8 \\ 19 \end{bmatrix} = \begin{bmatrix} 43 \\ 78 \end{bmatrix} \equiv \begin{bmatrix} 17 \\ 0 \end{bmatrix} \qquad K \begin{bmatrix} 22 \\ 0 \end{bmatrix} = \begin{bmatrix} 66 \\ 110 \end{bmatrix} \equiv \begin{bmatrix} 14 \\ 6 \end{bmatrix}$$

"It was a dark and stormy night."

IT WA SA DA RK AN DS TO RM YN IG HT

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$K \begin{bmatrix} 8 \\ 19 \end{bmatrix} = \begin{bmatrix} 43 \\ 78 \end{bmatrix} \equiv \begin{bmatrix} 17 \\ 0 \end{bmatrix} \qquad K \begin{bmatrix} 22 \\ 0 \end{bmatrix} = \begin{bmatrix} 66 \\ 110 \end{bmatrix} \equiv \begin{bmatrix} 14 \\ 6 \end{bmatrix}$$

$$K \begin{bmatrix} 18 \\ 0 \end{bmatrix} = \begin{bmatrix} 54 \\ 90 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 12 \end{bmatrix}$$

“It was a dark and stormy night.”

`IT WA SA DA RK AN DS TO RM YN IG HT`

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$K \begin{bmatrix} 8 \\ 19 \end{bmatrix} = \begin{bmatrix} 43 \\ 78 \end{bmatrix} \equiv \begin{bmatrix} 17 \\ 0 \end{bmatrix} \qquad K \begin{bmatrix} 22 \\ 0 \end{bmatrix} = \begin{bmatrix} 66 \\ 110 \end{bmatrix} \equiv \begin{bmatrix} 14 \\ 6 \end{bmatrix}$$

$$K \begin{bmatrix} 18 \\ 0 \end{bmatrix} = \begin{bmatrix} 54 \\ 90 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 12 \end{bmatrix} \qquad K \begin{bmatrix} 3 \\ 0 \end{bmatrix} = \begin{bmatrix} 9 \\ 15 \end{bmatrix} \equiv \begin{bmatrix} 9 \\ 15 \end{bmatrix}$$

"It was a dark and stormy night."

`IT WA SA DA RK AN DS TO RM YN IG HT`

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$K\begin{bmatrix}8\\19\end{bmatrix}=\begin{bmatrix}43\\78\end{bmatrix}\equiv\begin{bmatrix}17\\0\end{bmatrix} \qquad K\begin{bmatrix}22\\0\end{bmatrix}=\begin{bmatrix}66\\110\end{bmatrix}\equiv\begin{bmatrix}14\\6\end{bmatrix}$$

$$K\begin{bmatrix}18\\0\end{bmatrix}=\begin{bmatrix}54\\90\end{bmatrix}\equiv\begin{bmatrix}2\\12\end{bmatrix} \qquad K\begin{bmatrix}3\\0\end{bmatrix}=\begin{bmatrix}9\\15\end{bmatrix}\equiv\begin{bmatrix}9\\15\end{bmatrix}$$

17-00 14-06 02-12 09-15 09-01 13-00 01-25 19-19 11-05 07-16 04-00 14-21

"It was a dark and stormy night."

`IT WA SA DA RK AN DS TO RM YN IG HT`

08-19 22-00 18-00 03-00 17-10 00-13 03-18 19-14 17-12 24-13 08-06 07-19

$$K\begin{bmatrix}8\\19\end{bmatrix}=\begin{bmatrix}43\\78\end{bmatrix}\equiv\begin{bmatrix}17\\0\end{bmatrix}\qquad K\begin{bmatrix}22\\0\end{bmatrix}=\begin{bmatrix}66\\110\end{bmatrix}\equiv\begin{bmatrix}14\\6\end{bmatrix}$$

$$K\begin{bmatrix}18\\0\end{bmatrix}=\begin{bmatrix}54\\90\end{bmatrix}\equiv\begin{bmatrix}2\\12\end{bmatrix}\qquad K\begin{bmatrix}3\\0\end{bmatrix}=\begin{bmatrix}9\\15\end{bmatrix}\equiv\begin{bmatrix}9\\15\end{bmatrix}$$

17-00 14-06 02-12 09-15 09-01 13-00 01-25 19-19 11-05 07-16 04-00 14-21

`RA OG CM JP JA NA BZ TT LF HQ EA OV`

```
how are you today
how are you today

ZWS ENI USP LJVEU
```

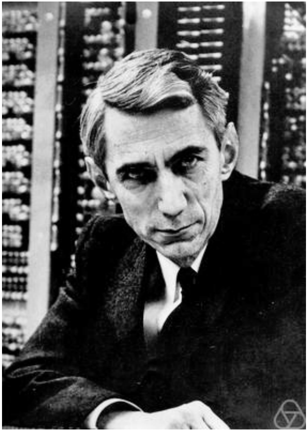
```
how are you today

ZWS ENI USP LJVEU
```

07-14 22-00 17-04 24-14 20-19 14-03 00-24 how are you today

ZWS ENI USP LJVEU

07-14 22-00 17-04 24-14 20-19 14-03 00-24

25-22 18-08 13-08 20-18 15-11 09-21 04-20



Claude Shannon

Picture CC BY-SA 2.0 de by Konrad Jacobs

Definition

An encryption method has good diffusion if changing one character of the plaintext changes several characters of the ciphertext, and vice versa.

Definition

An encryption method has good diffusion if changing one character of the plaintext changes several characters of the ciphertext, and vice versa.

Definition

An encryption method has good confusion if the key does not relate straightforwardly to the ciphertext, but each part of the ciphertext depends on many parts of the key.