BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

The Shift Cipher (cont)

A Caveat on Cracking The Shift Cipher

We used the following reasoning:

A Caveat on Cracking The Shift Cipher

We used the following reasoning:

1. $f_E \cdot f_E \sim 0.065$.
2. For $1 \leq i \leq 25$, f_i is English shifted by i. $f_E \cdot f_i \sim 0.035$.

A Caveat on Cracking The Shift Cipher

We used the following reasoning:

1. $f_E \cdot f_E \sim 0.065$.
2. For $1 \leq i \leq 25$, f_i is English shifted by i. $f_E \cdot f_i \sim 0.035$.
3. Find correct shift i by seeing which $f_E \cdot f_i$ is ~ 0.065.

A Caveat on Cracking The Shift Cipher

We used the following reasoning:

1. $f_E \cdot f_E \sim 0.065$.
2. For $1 \leq i \leq 25$, f_i is English shifted by i. $f_E \cdot f_i \sim 0.035$.
3. Find correct shift i by seeing which $f_E \cdot f_i$ is ~ 0.065.
4. Only one of the dot products will be close to 0.065.

A Caveat on Cracking The Shift Cipher

We used the following reasoning:

1. $f_E \cdot f_E \sim 0.065$.
2. For $1 \leq i \leq 25$, f_i is English shifted by i. $f_E \cdot f_i \sim 0.035$.
3. Find correct shift i by seeing which $f_E \cdot f_i$ is ~ 0.065.
4. Only one of the dot products will be close to 0.065.

Did we really need the numbers 0.068 and 0.035? Do we actually need them?

This will come up later in the course in a situation where finding the numbers is hard.

How we Would Crack Shift If Did Not Know Parameters 0.065, 0.035

Important point is that $f_E \cdot f_E$ is BIG, $f_E \cdot f_i$ SMALL. Do not need to know HOW BIG, HOW SMALL.

How we Would Crack Shift If Did Not Know Parameters 0.065, 0.035

Important point is that $f_E \cdot f_E$ is BIG, $f_E \cdot f_i$ SMALL. Do not need to know HOW BIG, HOW SMALL.

1. Input(T). T is a text that has been coded by the shift cipher.

How we Would Crack Shift If Did Not Know Parameters 0.065, 0.035

Important point is that $f_E \cdot f_E$ is BIG, $f_E \cdot f_i$ SMALL. Do not need to know HOW BIG, HOW SMALL.

1. Input(T). T is a text that has been coded by the shift cipher.
2. For $0 \leq i \leq 25$ find f_i, the freq vector of the T shifted by i.

How we Would Crack Shift If Did Not Know Parameters 0.065, 0.035

Important point is that $f_E \cdot f_E$ is BIG, $f_E \cdot f_i$ SMALL. Do not need to know HOW BIG, HOW SMALL.

1. Input(T). T is a text that has been coded by the shift cipher.
2. For $0 \leq i \leq 25$ find f_i, the freq vector of the T shifted by i.
3. Compute all $f_E \cdot f_i$. The i that has MAX of $f_E \cdot f_i$ is the i we want.

How we Would Crack Shift If Did Not Know Parameters 0.065, 0.035

Important point is that $f_E \cdot f_E$ is BIG, $f_E \cdot f_i$ SMALL. Do not need to know HOW BIG, HOW SMALL.

1. Input(T). T is a text that has been coded by the shift cipher.
2. For $0 \le i \le 25$ find f_i, the freq vector of the T shifted by i.
3. Compute all $f_E \cdot f_i$. The i that has MAX of $f_E \cdot f_i$ is the i we want.

Note Didn't need the parameters 0.065, 0.035 to do this.

How we Would Crack Shift If Did Not Know Parameters 0.065, 0.035

Important point is that $f_E \cdot f_E$ is BIG, $f_E \cdot f_i$ SMALL. Do not need to know HOW BIG, HOW SMALL.

1. Input(T). T is a text that has been coded by the shift cipher.
2. For $0 \le i \le 25$ find f_i, the freq vector of the T shifted by i.
3. Compute all $f_E \cdot f_i$. The i that has MAX of $f_E \cdot f_i$ is the i we want.

Note Didn't need the parameters 0.065, 0.035 to do this.

Downside Since we knew the parameters 0.065, 0.035 we knew there was a big gap. We knew there would be no close calls. If we do not know these kind of parameters then we are not as confident.

How we Would Crack Shift If Did Not Know Parameters 0.065, 0.035

Important point is that $f_E \cdot f_E$ is BIG, $f_E \cdot f_i$ SMALL. Do not need to know HOW BIG, HOW SMALL.

1. Input(T). T is a text that has been coded by the shift cipher.
2. For $0 \le i \le 25$ find f_i, the freq vector of the T shifted by i.
3. Compute all $f_E \cdot f_i$. The i that has MAX of $f_E \cdot f_i$ is the i we want.

Note Didn't need the parameters 0.065, 0.035 to do this.

Downside Since we knew the parameters 0.065, 0.035 we knew there was a big gap. We knew there would be no close calls. If we do not know these kind of parameters then we are not as confident.

But if we have a few candidates for IS-ENGLISH there may be other ways to pick out the real one.

Variants of the Shift Cipher

What About Texts With Numbers?

We have discussed English texts with $\Sigma = \{a, \ldots, z\}$.

What About Texts With Numbers?

We have discussed English texts with $\Sigma = \{a, \ldots, z\}$.

What if the text has numbers in it? Examples:

What About Texts With Numbers?

We have discussed English texts with $\Sigma = \{a, \ldots, z\}$.

What if the text has numbers in it? Examples:

1. Financial Documents. $\Sigma = \{a, b, \ldots, z, 0, \ldots, 9\}$.

What About Texts With Numbers?

We have discussed English texts with $\Sigma = \{a, \ldots, z\}$.

What if the text has numbers in it? Examples:

1. Financial Documents. $\Sigma = \{a, b, \ldots, z, 0, \ldots, 9\}$.
2. Math books such as:
   `https://www.amazon.com/Mathematical-Muffin-Morsels-Problem-Mathematics/dp/9811215979/ref=sr_1_2?dchild=1&keywords=gasarch&qid=1593879329&sr=8-2`

   $$\Sigma = \{a, \ldots, z, 0, \ldots, 9, +, \times, -, \div, =, \equiv, <, >, \cap, \cup, \emptyset\}$$

   Include other symbols depending on the branch of math. E.g., $\wedge, \vee$ for logic.

What About Texts With Numbers?

We have discussed English texts with $\Sigma = \{a, \ldots, z\}$.

What if the text has numbers in it? Examples:

1. Financial Documents. $\Sigma = \{a, b, \ldots, z, 0, \ldots, 9\}$.
2. Math books such as:
   https://www.amazon.com/Mathematical-Muffin-Morsels-Problem-Mathematics/dp/9811215979/ref=sr_1_2?dchild=1&keywords=gasarch&qid=1593879329&sr=8-2

   $$\Sigma = \{a, \ldots, z, 0, \ldots, 9, +, \times, -, \div, =, \equiv, <, >, \cap, \cup, \emptyset\}$$

   Include other symbols depending on the branch of math. E.g., $\wedge, \vee$ for logic.

What to do? Find distribution of alphabet for these types of docs. Write code sim to **Is-English** and try all shifts.

Is Shift Cipher Secure if we are Transmitting Just Numbers?

What if Alice sends Bob a credit card number? **Discuss**

Is Shift Cipher Secure if we are Transmitting Just Numbers?

What if Alice sends Bob a credit card number? **Discuss**
Credit Card Numbers also have patterns:

Is Shift Cipher Secure if we are Transmitting Just Numbers?

What if Alice sends Bob a credit card number? **Discuss**
Credit Card Numbers also have patterns:

1. Visa cards always begin with 4.

Is Shift Cipher Secure if we are Transmitting Just Numbers?

What if Alice sends Bob a credit card number? **Discuss**
Credit Card Numbers also have patterns:

1. Visa cards always begin with 4.
2. American Express always begins 34 or 37.

Is Shift Cipher Secure if we are Transmitting Just Numbers?

What if Alice sends Bob a credit card number? **Discuss**
Credit Card Numbers also have patterns:

1. Visa cards always begin with 4.
2. American Express always begins 34 or 37.
3. Mastercard starts with 51 or 52 or 53 or 54.

Is Shift Cipher Secure if we are Transmitting Just Numbers?

What if Alice sends Bob a credit card number? **Discuss**
Credit Card Numbers also have patterns:

1. Visa cards always begin with 4.
2. American Express always begins 34 or 37.
3. Mastercard starts with 51 or 52 or 53 or 54.
4. Parity Checks.

Byte-wise Shift Cipher

- In ASCII all small letters, cap letters, numbers, punctuation, mapped to 8-bit strings.
- Use XOR instead of modular addition. Fast!
- Decode and Encode are both XOR.
- Essential properties still hold.

Hex	Dec	Char		Hex	Dec	Char	Hex	Dec	Char	Hex	Dec	Char
0x00	0	NULL	null	0x20	32	Space	0x40	64	@	0x60	96	`
0x01	1	SOH	Start of heading	0x21	33	!	0x41	65	A	0x61	97	a
0x02	2	STX	Start of text	0x22	34	"	0x42	66	B	0x62	98	b
0x03	3	ETX	End of text	0x23	35	#	0x43	67	C	0x63	99	c
0x04	4	EOT	End of transmission	0x24	36	$	0x44	68	D	0x64	100	d
0x05	5	ENQ	Enquiry	0x25	37	%	0x45	69	E	0x65	101	e
0x06	6	ACK	Acknowledge	0x26	38	&	0x46	70	F	0x66	102	f
0x07	7	BELL	Bell	0x27	39	'	0x47	71	G	0x67	103	g
0x08	8	BS	Backspace	0x28	40	(	0x48	72	H	0x68	104	h
0x09	9	TAB	Horizontal tab	0x29	41	)	0x49	73	I	0x69	105	i
0x0A	10	LF	New line	0x2A	42	*	0x4A	74	J	0x6A	106	j
0x0B	11	VT	Vertical tab	0x2B	43	+	0x4B	75	K	0x6B	107	k
0x0C	12	FF	Form Feed	0x2C	44	,	0x4C	76	L	0x6C	108	l
0x0D	13	CR	Carriage return	0x2D	45	-	0x4D	77	M	0x6D	109	m
0x0E	14	SO	Shift out	0x2E	46	.	0x4E	78	N	0x6E	110	n
0x0F	15	SI	Shift in	0x2F	47	/	0x4F	79	O	0x6F	111	o
0x10	16	DLE	Data link escape	0x30	48	0	0x50	80	P	0x70	112	p
0x11	17	DC1	Device control 1	0x31	49	1	0x51	81	Q	0x71	113	q
0x12	18	DC2	Device control 2	0x32	50	2	0x52	82	R	0x72	114	r
0x13	19	DC3	Device control 3	0x33	51	3	0x53	83	S	0x73	115	s
0x14	20	DC4	Device control 4	0x34	52	4	0x54	84	T	0x74	116	t
0x15	21	NAK	Negative ack	0x35	53	5	0x55	85	U	0x75	117	u
0x16	22	SYN	Synchronous idle	0x36	54	6	0x56	86	V	0x76	118	v
0x17	23	ETB	End transmission block	0x37	55	7	0x57	87	W	0x77	119	w
0x18	24	CAN	Cancel	0x38	56	8	0x58	88	X	0x78	120	x
0x19	25	EM	End of medium	0x39	57	9	0x59	89	Y	0x79	121	y
0x1A	26	SUB	Substitute	0x3A	58	:	0x5A	90	Z	0x7A	122	z
0x1B	27	FSC	Escape	0x3B	59	;	0x5B	91	[	0x7B	123	{
0x1C	28	FS	File separator	0x3C	60	<	0x5C	92	\	0x7C	124	|
0x1D	29	GS	Group separator	0x3D	61	=	0x5D	93	]	0x7D	125	}
0x1E	30	RS	Record separator	0x3E	62	>	0x5E	94	^	0x7E	126	~
0x1F	31	US	Unit separator	0x3F	63	?	0x5F	95	_	0x7F	127	DEL

Source: http://benborowiec.com/2011/07/23/better-ascii-table/

Byte-wise shift cipher

- $\mathcal{M} = \{\text{strings of bytes}\}$

Byte-wise shift cipher

- $\mathcal{M} = \{\text{strings of bytes}\}$
- *Gen*: choose uniform byte $k \in \mathcal{K} = \{0, \ldots, 255\}$

Byte-wise shift cipher

- $\mathcal{M} = \{\text{strings of bytes}\}$
- *Gen*: choose uniform byte $k \in \mathcal{K} = \{0, \ldots, 255\}$
- $Enc_k(m_1 \ldots m_t)$: output $c_1 \ldots c_t$, where $c_i \leftarrow m_i \oplus k$

Byte-wise shift cipher

- $\mathcal{M} = \{\text{strings of bytes}\}$
- *Gen*: choose uniform byte $k \in \mathcal{K} = \{0, \ldots, 255\}$
- $Enc_k(m_1 \ldots m_t)$: output $c_1 \ldots c_t$, where $c_i \leftarrow m_i \oplus k$
- $Dec_k(c_1 \ldots c_t)$: output $m_1 \ldots m_t$, where $m_i \leftarrow c_i \oplus k$

Byte-wise shift cipher

- $\mathcal{M} = \{\text{strings of bytes}\}$
- *Gen*: choose uniform byte $k \in \mathcal{K} = \{0,\ldots,255\}$
- $Enc_k(m_1 \ldots m_t)$: output $c_1 \ldots c_t$, where $c_i \leftarrow m_i \oplus k$
- $Dec_k(c_1 \ldots c_t)$: output $m_1 \ldots m_t$, where $m_i \leftarrow c_i \oplus k$
- Verify that correctness holds.

Byte-wise shift cipher

- $\mathcal{M}$ = {strings of bytes}
- *Gen*: choose uniform byte $k \in \mathcal{K} = \{0,\ldots,255\}$
- $Enc_k(m_1 \ldots m_t)$: output $c_1 \ldots c_t$, where $c_i \leftarrow m_i \oplus k$
- $Dec_k(c_1 \ldots c_t)$: output $m_1 \ldots m_t$, where $m_i \leftarrow c_i \oplus k$
- Verify that correctness holds.
- Curiosity: Encrypt and Decrypt Key are the same.

Example

Key is $\mathbf{11001110}$.
Alice wants to send $\mathbf{00011010}, \mathbf{11100011}, \mathbf{00000000}$.
She sends
$\mathbf{00011010} \oplus \mathbf{11001110}$
$\mathbf{11100011} \oplus \mathbf{11001110}$
$\mathbf{00000000} \oplus \mathbf{11001110}$

$$= 11010100, 00101101, 11001110$$

Example

Key is $\mathbf{11001110}$.
Alice wants to send $\mathbf{00011010}, \mathbf{11100011}, \mathbf{00000000}$.
She sends
$\mathbf{00011010} \oplus \mathbf{11001110}$
$\mathbf{11100011} \oplus \mathbf{11001110}$
$\mathbf{00000000} \oplus \mathbf{11001110}$

$$= 11010100, 00101101, 11001110$$

Question: Should it worry Alice and Bob that the key itself was transmitted? **Discuss**

Example

Key is $\mathbf{11001110}$.

Alice wants to send $\mathbf{00011010}, \mathbf{11100011}, \mathbf{00000000}$.

She sends

$\mathbf{00011010} \oplus \mathbf{11001110}$

$\mathbf{11100011} \oplus \mathbf{11001110}$

$\mathbf{00000000} \oplus \mathbf{11001110}$

$$= 11010100, 00101101, 11001110$$

Question: Should it worry Alice and Bob that the key itself was transmitted? **Discuss**

No. Eve has no way of knowing that.

Is this Cipher Secure?

- Today NO—only 256 possible keys!

Is this Cipher Secure?

- Today NO—only 256 possible keys!
- 100 years ago might have been secure.

Is this Cipher Secure?

- Today NO—only 256 possible keys!
- 100 years ago might have been secure.
- Given a ciphertext, try decrypting with every possible key.

Is this Cipher Secure?

- Today NO—only 256 possible keys!
- 100 years ago might have been secure.
- Given a ciphertext, try decrypting with every possible key.
- If ciphertext is long enough, only one plaintext will **look like English**.

Is this Cipher Secure?

- Today NO—only 256 possible keys!
- 100 years ago might have been secure.
- Given a ciphertext, try decrypting with every possible key.
- If ciphertext is long enough, only one plaintext will **look like English**.

What is more secure: 26-letter shift or the 256-keys Byte Shift.

Is this Cipher Secure?

- Today NO—only 256 possible keys!
- 100 years ago might have been secure.
- Given a ciphertext, try decrypting with every possible key.
- If ciphertext is long enough, only one plaintext will **look like English**.

What is more secure: 26-letter shift or the 256-keys Byte Shift.

- Byte is more secure- More Keys.

Is this Cipher Secure?

- Today NO—only 256 possible keys!
- 100 years ago might have been secure.
- Given a ciphertext, try decrypting with every possible key.
- If ciphertext is long enough, only one plaintext will **look like English**.

What is more secure: 26-letter shift or the 256-keys Byte Shift.

- Byte is more secure- More Keys.
- Byte is less secure- uses punctuation which yields more patterns.

Is this Cipher Secure?

- Today NO—only 256 possible keys!
- 100 years ago might have been secure.
- Given a ciphertext, try decrypting with every possible key.
- If ciphertext is long enough, only one plaintext will **look like English**.

What is more secure: 26-letter shift or the 256-keys Byte Shift.

- Byte is more secure- More Keys.
- Byte is less secure- uses punctuation which yields more patterns.
- I do not know the answer.

Sufficient Key Space Principle

- The key space must be large enough to make exhaustive-search attacks impractical.
  - How large this is may be technology-dependent.

Sufficient Key Space Principle

- The key space must be large enough to make exhaustive-search attacks impractical.
  - How large this is may be technology-dependent.
- Note: this makes some assumptions...
  - English-language plaintext
  - Ciphertext sufficiently long so only one valid plaintext

Kerckhoff's Principle

Kerckhoff's principle

We made the comment **We KNOW that SHIFT was used.**
More generally we will always use the following assumption.
Kerckhoff's principle:

- Eve knows **The encryption scheme**.
- Eve knows **the alphabet and the language**.
- Eve does not know **the key**
- The key is chosen **at random**.

Arguments For And Against Kerckhoff's Principle

Arguments For:

- Easier to keep *key* secret than *algorithm*.
- Easier to change *key* than to change *algorithm*.
- Standardization:
  - Ease of deployment.
  - Public validation.
- If prove system secure then very strong proof of security since even if Eve knows scheme she can't crack.

Arguments For And Against Kerckhoff's Principle

Arguments For:

- Easier to keep *key* secret than *algorithm*.
- Easier to change *key* than to change *algorithm*.
- Standardization:
  - Ease of deployment.
  - Public validation.
- If prove system secure then very strong proof of security since even if Eve knows scheme she can't crack.

Arguments Against:

- The first few years (months? days? hours?) of a new type of cipher, perhaps you can use that Eve does not know it. But she will soon!

Formal Security with Shift Cipher as Example

1-Letter Shift Cipher

Odd Situation What if message is only one-letter long?
Discuss Can Eve crack a one-letter message?

1-Letter Shift Cipher

Odd Situation What if message is only one-letter long?
Discuss Can Eve crack a one-letter message?
Intuitively No Eve cannot crack it.

1-Letter Shift Cipher

Odd Situation What if message is only one-letter long?
Discuss Can Eve crack a one-letter message?
Intuitively No Eve cannot crack it. This is correct.

1-Letter Shift Cipher

Odd Situation What if message is only one-letter long?
Discuss Can Eve crack a one-letter message?
Intuitively No Eve cannot crack it. This is correct.
Discuss How to define **secure**?

TE Means Thought Experiment

We are going to do Thought Experiments.

TE Means Thought Experiment

We are going to do Thought Experiments.

For reasons of space I call them TE.

Convention

- $m \in \{x, y\}$ is the message Alice wants to send
- $s \in \{0, 1\}$ is the shift.
- $c \in \{x, y\}$ is what Alice sends.

The statement

$$\textit{Alice sends } m + s$$

means that that Alice sends m shifted by s (with wrap around).

Convention

- $m \in \{x, y\}$ is the message Alice wants to send
- $s \in \{0, 1\}$ is the shift.
- $c \in \{x, y\}$ is what Alice sends.

The statement

$$\textit{Alice sends } m + s$$

means that that Alice sends m shifted by s (with wrap around).

m	s	c
x	0	x
x	1	y
y	0	y
y	1	x

(TE1) $\{x, y\}$, Equally Likely; Shift 0,1 Equally Likely

$\Pr(m = x) = \Pr(m = y) = \frac{1}{2}$. $\Pr(s = 0) = \Pr(s = 1) = \frac{1}{2}$.

(TE1) $\{x, y\}$, Equally Likely; Shift 0,1 Equally Likely

$\Pr(m = x) = \Pr(m = y) = \frac{1}{2}$. $\Pr(s = 0) = \Pr(s = 1) = \frac{1}{2}$.

m	s	c	$\Pr$
x	0	x	$1/4$
x	1	y	$1/4$
y	0	y	$1/4$
y	1	x	$1/4$

(TE1) $\{x, y\}$, Equally Likely; Shift 0,1 Equally Likely

$\Pr(m = x) = \Pr(m = y) = \frac{1}{2}$. $\Pr(s = 0) = \Pr(s = 1) = \frac{1}{2}$.

m	s	c	$\Pr$
x	0	x	$1/4$
x	1	y	$1/4$
y	0	y	$1/4$
y	1	x	$1/4$

Before Alice sends $c = m + s$ Eve knows:

(TE1) $\{x, y\}$, Equally Likely; Shift 0,1 Equally Likely

$\Pr(m = x) = \Pr(m = y) = \frac{1}{2}$. $\Pr(s = 0) = \Pr(s = 1) = \frac{1}{2}$.

m	s	c	$\Pr$
x	0	x	$1/4$
x	1	y	$1/4$
y	0	y	$1/4$
y	1	x	$1/4$

Before Alice sends $c = m + s$ Eve knows:

$$\Pr(m = x) = \frac{1}{2}, \Pr(m = y) = \frac{1}{2}$$

(TE1) $\{x, y\}$, Equally Likely; Shift 0,1 Equally Likely

$\Pr(m = x) = \Pr(m = y) = \frac{1}{2}$. $\Pr(s = 0) = \Pr(s = 1) = \frac{1}{2}$.

m	s	c	$\Pr$
x	0	x	$1/4$
x	1	y	$1/4$
y	0	y	$1/4$
y	1	x	$1/4$

Before Alice sends $c = m + s$ Eve knows:

$$\Pr(m = x) = \frac{1}{2}, \Pr(m = y) = \frac{1}{2}$$

Eve sees $c = x$. Now what does she know?

m	s	c	$\Pr$ Not Normalized	$\Pr$ Normalized
x	0	x	$1/4$	$1/2$
y	1	x	$1/4$	$1/2$

(TE1) $\{x, y\}$, Equally Likely; Shift 0,1 Equally Likely

$\Pr(m = x) = \Pr(m = y) = \frac{1}{2}$. $\Pr(s = 0) = \Pr(s = 1) = \frac{1}{2}$.

m	s	c	$\Pr$
x	0	x	$1/4$
x	1	y	$1/4$
y	0	y	$1/4$
y	1	x	$1/4$

Before Alice sends $c = m + s$ Eve knows:

$$\Pr(m = x) = \frac{1}{2}, \Pr(m = y) = \frac{1}{2}$$

Eve sees $c = x$. Now what does she know?

m	s	c	$\Pr$ Not Normalized	$\Pr$ Normalized
x	0	x	$1/4$	$1/2$
y	1	x	$1/4$	$1/2$

Eve learned **nothing** from seeing c. Intuitively this means **secure**.

(TE2) Alphabet $\{x, y\}$, Unequal Prob

$\Pr(m = x) = \frac{1}{4}$; $\Pr(m = y) = \frac{3}{4}$. $\Pr(s = 0) = \frac{1}{2}$; $\Pr(s = 1) = \frac{1}{2}$.

m	s	c	$\Pr$
x	0	x	$1/8$
x	1	y	$1/8$
y	0	y	$3/8$
y	1	x	$3/8$

Before Alice sees $c = m + s$ Eve knows:

$$\Pr(m = x) = \frac{1}{4}, \Pr(m = y) = \frac{3}{4}$$

(TE2) Alphabet $\{x, y\}$, Unequal Prob

$\Pr(m = x) = \frac{1}{4}$; $\Pr(m = y) = \frac{3}{4}$. $\Pr(s = 0) = \frac{1}{2}$; $\Pr(s = 1) = \frac{1}{2}$.

m	s	c	$\Pr$
x	0	x	1/8
x	1	y	1/8
y	0	y	3/8
y	1	x	3/8

Before Alice sees $c = m + s$ Eve knows:

$$\Pr(m = x) = \frac{1}{4}, \Pr(m = y) = \frac{3}{4}$$

Eve sees $c = x$. Now what does she know?

(TE2) Alphabet $\{x, y\}$, Unequal Prob

$\Pr(m = x) = \frac{1}{4}$; $\Pr(m = y) = \frac{3}{4}$. $\Pr(s = 0) = \frac{1}{2}$; $\Pr(s = 1) = \frac{1}{2}$.

m	s	c	$\Pr$
x	0	x	$1/8$
x	1	y	$1/8$
y	0	y	$3/8$
y	1	x	$3/8$

Before Alice sees $c = m + s$ Eve knows:

$$\Pr(m = x) = \frac{1}{4}, \Pr(m = y) = \frac{3}{4}$$

Eve sees $c = x$. Now what does she know?

m	s	c	$\Pr$ Not Normalized	$\Pr$ Normalized
x	0	x	$1/8$	$1/4$
y	1	x	$3/8$	$3/4$

(TE2) Alphabet $\{x, y\}$, Unequal Prob

$\Pr(m = x) = \frac{1}{4}$; $\Pr(m = y) = \frac{3}{4}$. $\Pr(s = 0) = \frac{1}{2}$; $\Pr(s = 1) = \frac{1}{2}$.

m	s	c	$\Pr$
x	0	x	1/8
x	1	y	1/8
y	0	y	3/8
y	1	x	3/8

Before Alice sees $c = m + s$ Eve knows:

$$\Pr(m = x) = \frac{1}{4}, \Pr(m = y) = \frac{3}{4}$$

Eve sees $c = x$. Now what does she know?

m	s	c	$\Pr$ Not Normalized	$\Pr$ Normalized
x	0	x	1/8	1/4
y	1	x	3/8	3/4

Eve learned **nothing** from seeing m. Intuitively this means **secure**.

(TE3) Alphabet $\{x, y\}$, Equal Prob, Shift Biased

$\Pr(m = x) = \frac{1}{2}$; $\Pr(m = y) = \frac{1}{2}$. $\Pr(s = 0) = \frac{1}{4}$, $\Pr(s = 1) = \frac{3}{4}$.

(TE3) Alphabet $\{x, y\}$, Equal Prob, Shift Biased

$\Pr(m = x) = \frac{1}{2}$; $\Pr(m = y) = \frac{1}{2}$. $\Pr(s = 0) = \frac{1}{4}$, $\Pr(s = 1) = \frac{3}{4}$.

m	s	c	$\Pr$
x	0	x	$1/8$
x	1	y	$3/8$
y	0	y	$1/8$
y	1	x	$3/8$

Before Alice sends $c = m + s$ Eve knows:

(TE3) Alphabet $\{x, y\}$, Equal Prob, Shift Biased

$\Pr(m = x) = \frac{1}{2}$; $\Pr(m = y) = \frac{1}{2}$. $\Pr(s = 0) = \frac{1}{4}$, $\Pr(s = 1) = \frac{3}{4}$.

m	s	c	$\Pr$
x	0	x	1/8
x	1	y	3/8
y	0	y	1/8
y	1	x	3/8

Before Alice sends $c = m + s$ Eve knows:

Eve sees $c = x$. Now what does she know?

$$\Pr(m = x) = \frac{1}{2}; \Pr(m = y) = \frac{1}{2}$$

(TE3) Alphabet $\{x, y\}$, Equal Prob, Shift Biased

$\Pr(m = x) = \frac{1}{2}$; $\Pr(m = y) = \frac{1}{2}$. $\Pr(s = 0) = \frac{1}{4}$, $\Pr(s = 1) = \frac{3}{4}$.

m	s	c	$\Pr$
x	0	x	1/8
x	1	y	3/8
y	0	y	1/8
y	1	x	3/8

Before Alice sends $c = m + s$ Eve knows:

Eve sees $c = x$. Now what does she know?

$$\Pr(m = x) = \frac{1}{2}; \Pr(m = y) = \frac{1}{2}$$

Eve sees $c = x$. Now what does she know?

m	s	c	$\Pr$ Not Normalized	$\Pr$ Normalized
x	0	x	1/8	1/4
y	1	x	3/8	3/4

(TE3) Alphabet $\{x, y\}$, Equal Prob, Shift Biased

$\Pr(m = x) = \frac{1}{2}$; $\Pr(m = y) = \frac{1}{2}$. $\Pr(s = 0) = \frac{1}{4}$, $\Pr(s = 1) = \frac{3}{4}$.

m	s	c	$\Pr$
x	0	x	1/8
x	1	y	3/8
y	0	y	1/8
y	1	x	3/8

Before Alice sends $c = m + s$ Eve knows:

Eve sees $c = x$. Now what does she know?

$$\Pr(m = x) = \frac{1}{2}; \Pr(m = y) = \frac{1}{2}$$

Eve sees $c = x$. Now what does she know?

m	s	c	$\Pr$ Not Normalized	$\Pr$ Normalized
x	0	x	1/8	1/4
y	1	x	3/8	3/4

Before: Eve-$\Pr(m = x) = \frac{1}{2}$. After: Eve $\Pr(m = x) = \frac{1}{4}$.

Eve has learned something !

BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

Upshot

Upshot

- **Insecure** does not mean Eve can find the message.

Upshot

- **Insecure** does not mean Eve can find the message.
- **Insecure** means that Eve knows more **after** seeing c than she did **before** seeing c.

Upshot

- **Insecure** does not mean Eve can find the message.
- **Insecure** means that Eve knows more **after** seeing c than she did **before** seeing c.
- What she knows might involve probability.

Upshot

- **Insecure** does not mean Eve can find the message.
- **Insecure** means that Eve knows more **after** seeing c than she did **before** seeing c.
- What she knows might involve probability.
- We need to make this all more rigorous!

We Need Conditional Probability

Conditional probability Probability that one event occurs, *given that some other event occurred.*

We Need Conditional Probability

Conditional probability Probability that one event occurs, *given that some other event occurred.*

Notation $\Pr(A|B)$.

We Need Conditional Probability

Conditional probability Probability that one event occurs, *given that some other event occurred.*

Notation $\Pr(A|B)$.

Formal Definition Notation $\Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)}$.

We Need Conditional Probability

Conditional probability Probability that one event occurs, *given that some other event occurred.*

Notation $\Pr(A|B)$.

Formal Definition Notation $\Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)}$.
Intuition $\Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)}$ is saying that the entire space is now $\Pr(B)$. Within that space what is the prob of A happening? Its $\Pr(A \cap B)$.

Examples of Conditional Probability

Josh rolls dice d_1, d_2 and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$?

Examples of Conditional Probability

Josh rolls dice d_1, d_2 and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$? $\frac{1}{9}$.
What if you know d_1?

Examples of Conditional Probability

Josh rolls dice d_1, d_2 and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$? $\frac{1}{9}$.
What if you know d_1?
$\Pr(s = 5 | d_1 = 1) = \frac{\Pr(s=5 \wedge d_1=1)}{\Pr(d_1=1)} = \frac{1/36}{1/6} = \frac{1}{6}$.

Examples of Conditional Probability

Josh rolls dice d_1, d_2 and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$? $\frac{1}{9}$.
What if you know d_1?

$\Pr(s = 5 | d_1 = 1) = \frac{\Pr(s=5 \wedge d_1=1)}{\Pr(d_1=1)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5 | d_1 = 2) = \frac{\Pr(s=5 \wedge d_1=2)}{\Pr(d_1=2)} = \frac{1/36}{1/6} = \frac{1}{6}$.

Examples of Conditional Probability

Josh rolls dice d_1, d_2 and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$? $\frac{1}{9}$.
What if you know d_1?

$\Pr(s = 5 | d_1 = 1) = \frac{\Pr(s=5 \wedge d_1=1)}{\Pr(d_1=1)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5 | d_1 = 2) = \frac{\Pr(s=5 \wedge d_1=2)}{\Pr(d_1=2)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5 | d_1 = 3) = \frac{\Pr(s=5 \wedge d_1=3)}{\Pr(d_1=3)} = \frac{1/36}{1/6} = \frac{1}{6}$.

Examples of Conditional Probability

Josh rolls dice d_1, d_2 and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$? $\frac{1}{9}$.
What if you know d_1?

$\Pr(s = 5 | d_1 = 1) = \frac{\Pr(s=5 \wedge d_1=1)}{\Pr(d_1=1)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5 | d_1 = 2) = \frac{\Pr(s=5 \wedge d_1=2)}{\Pr(d_1=2)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5 | d_1 = 3) = \frac{\Pr(s=5 \wedge d_1=3)}{\Pr(d_1=3)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5 | d_1 = 4) = \frac{\Pr(s=5 \wedge d_1=4)}{\Pr(d_1=4)} = \frac{1/36}{1/6} = \frac{1}{6}$.

Examples of Conditional Probability

Josh rolls dice d_1, d_2 and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$? $\frac{1}{9}$.
What if you know d_1?

$\Pr(s = 5 | d_1 = 1) = \frac{\Pr(s=5 \wedge d_1=1)}{\Pr(d_1=1)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5 | d_1 = 2) = \frac{\Pr(s=5 \wedge d_1=2)}{\Pr(d_1=2)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5 | d_1 = 3) = \frac{\Pr(s=5 \wedge d_1=3)}{\Pr(d_1=3)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5 | d_1 = 4) = \frac{\Pr(s=5 \wedge d_1=4)}{\Pr(d_1=4)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5 | d_1 = 5) = \frac{\Pr(s=5 \wedge d_1=5)}{\Pr(d_1=5)} = \frac{0}{1/6} = 0$.

Examples of Conditional Probability

Josh rolls dice d_1, d_2 and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$? $\frac{1}{9}$.
What if you know d_1?

$\Pr(s = 5|d_1 = 1) = \frac{\Pr(s=5 \wedge d_1=1)}{\Pr(d_1=1)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5|d_1 = 2) = \frac{\Pr(s=5 \wedge d_1=2)}{\Pr(d_1=2)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5|d_1 = 3) = \frac{\Pr(s=5 \wedge d_1=3)}{\Pr(d_1=3)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5|d_1 = 4) = \frac{\Pr(s=5 \wedge d_1=4)}{\Pr(d_1=4)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5|d_1 = 5) = \frac{\Pr(s=5 \wedge d_1=5)}{\Pr(d_1=5)} = \frac{0}{1/6} = 0$.

$\Pr(s = 5|d_1 = 6) = \frac{\Pr(s=5 \wedge d_1=6)}{\Pr(d_1=6)} = \frac{0}{1/6} = 0$.

Examples of Conditional Probability

Josh rolls dice d_1, d_2 and finds $s = d_1 + d_2$. What is $\Pr(s = 5)$? $\frac{1}{9}$.
What if you know d_1?

$\Pr(s = 5|d_1 = 1) = \frac{\Pr(s=5 \wedge d_1=1)}{\Pr(d_1=1)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5|d_1 = 2) = \frac{\Pr(s=5 \wedge d_1=2)}{\Pr(d_1=2)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5|d_1 = 3) = \frac{\Pr(s=5 \wedge d_1=3)}{\Pr(d_1=3)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5|d_1 = 4) = \frac{\Pr(s=5 \wedge d_1=4)}{\Pr(d_1=4)} = \frac{1/36}{1/6} = \frac{1}{6}$.

$\Pr(s = 5|d_1 = 5) = \frac{\Pr(s=5 \wedge d_1=5)}{\Pr(d_1=5)} = \frac{0}{1/6} = 0$.

$\Pr(s = 5|d_1 = 6) = \frac{\Pr(s=5 \wedge d_1=6)}{\Pr(d_1=6)} = \frac{0}{1/6} = 0$.

This example is bad since, for example
$\Pr(s = 5|d_1 = 2) = \Pr(d_2 = 3) = \frac{1}{6}$.
$\Pr(s = 5|d_1 = 5) = \Pr(d_2 = 0) = 0$.

Conditional Probability Example with Mods and Dice

Josh rolls die d and announces the parity.

Conditional Probability Example with Mods and Dice

Josh rolls die d and announces the parity.

$\Pr(d = 1 | d \text{ even}) = \frac{\Pr(d=1 \wedge d\equiv 0)}{\Pr(d\equiv 1)} = 0$

Conditional Probability Example with Mods and Dice

Josh rolls die d and announces the parity.

$\Pr(d = 1 | d \text{ even}) = \frac{\Pr(d=1 \wedge d \equiv 0)}{\Pr(d \equiv 1)} = 0$

$\Pr(d = 1 | d \text{ odd}) = \frac{\Pr(d=1 \wedge d \equiv 1)}{\Pr(d \equiv 1)} = \frac{1/6}{1/2} = \frac{1}{3}$

Conditional Probability Example with Mods and Dice

Josh rolls die d and announces the parity.

$\Pr(d = 1|d \text{ even}) = \frac{\Pr(d=1 \wedge d \equiv 0)}{\Pr(d \equiv 1)} = 0$

$\Pr(d = 1|d \text{ odd}) = \frac{\Pr(d=1 \wedge d \equiv 1)}{\Pr(d \equiv 1)} = \frac{1/6}{1/2} = \frac{1}{3}$

The rest are similar and are always either 0 or $\frac{1}{3}$.

Conditional Probability Example with Funky Dice

Josh rolls two dice d_1, d_2 and finds $s = d_1 + d_2$.
The dice are **not** independent.
d_1 is fair.
If d_1 is i, then $d_2 \le i$, but within that equal prob.
If $d_1 = 3$ then d_2 is 1,2,3 each with prob $\frac{1}{3}$.

Conditional Probability Example with Funky Dice

Josh rolls two dice d_1, d_2 and finds $s = d_1 + d_2$.
The dice are **not** independent.
d_1 is fair.
If d_1 is i, then $d_2 \leq i$, but within that equal prob.
If $d_1 = 3$ then d_2 is 1,2,3 each with prob $\frac{1}{3}$.
Shortcut $\Pr(d_1 = i \wedge s = 5) = \Pr(d_1 = i \wedge d_2 = 5 - i)$.

Conditional Probability Example with Funky Dice

Josh rolls two dice d_1, d_2 and finds $s = d_1 + d_2$.
The dice are **not** independent.
d_1 is fair.
If d_1 is i, then $d_2 \le i$, but within that equal prob.
If $d_1 = 3$ then d_2 is 1,2,3 each with prob $\frac{1}{3}$.

Shortcut $\Pr(d_1 = i \wedge s = 5) = \Pr(d_1 = i \wedge d_2 = 5 - i)$.

$$\Pr(s = 5 | d_1 = 1) = \frac{\Pr(d_1{=}1 \wedge d_2{=}4)}{\Pr(d_1{=}1)} = 0$$

$$\Pr(s = 5 | d_1 = 2) = \frac{\Pr(d_1{=}2 \wedge d_2{=}3)}{\Pr(d_1{=}2)} = 0$$

$$\Pr(s = 5 | d_1 = 3) = \frac{\Pr(d_1{=}3 \wedge d_2{=}2)}{\Pr(d_1{=}3)} = \frac{1/6 \times 1/3}{1/6} = \frac{1}{3}.$$

$$\Pr(s = 5 | d_1 = 4) = \frac{\Pr(d_1{=}4 \wedge d_2{=}1)}{\Pr(d_1{=}4)} = \frac{1/6 \times 1/4}{1/6} = \frac{1}{4}.$$

$$\Pr(s = 5 | d_1 = 5) = \frac{\Pr(d_1{=}5 \wedge d_2{=}0)}{\Pr(d_1{=}5)} = 0.$$

$$\Pr(s = 5 | d_1 = 6) = \frac{\Pr(d_1{=}5 \wedge d_2{=}-1)}{\Pr(d_1{=}6)} = 0.$$

Conditional Probability Example with Funky Dice

Josh rolls two dice d_1, d_2 and finds $s = d_1 + d_2$.
The dice are **not** independent.
d_1 is fair.
If d_1 is i, then $d_2 \le i$, but within that equal prob.
If $d_1 = 3$ then d_2 is 1,2,3 each with prob $\frac{1}{3}$.

Shortcut $\Pr(d_1 = i \wedge s = 5) = \Pr(d_1 = i \wedge d_2 = 5 - i)$.

$\Pr(s = 5 | d_1 = 1) = \frac{\Pr(d_1=1 \wedge d_2=4)}{\Pr(d_1=1)} = 0$

$\Pr(s = 5 | d_1 = 2) = \frac{\Pr(d_1=2 \wedge d_2=3)}{\Pr(d_1=2)} = 0$

$\Pr(s = 5 | d_1 = 3) = \frac{\Pr(d_1=3 \wedge d_2=2)}{\Pr(d_1=3)} = \frac{1/6 \times 1/3}{1/6} = \frac{1}{3}$.

$\Pr(s = 5 | d_1 = 4) = \frac{\Pr(d_1=4 \wedge d_2=1)}{\Pr(d_1=4)} = \frac{1/6 \times 1/4}{1/6} = \frac{1}{4}$.

$\Pr(s = 5 | d_1 = 5) = \frac{\Pr(d_1=5 \wedge d_2=0)}{\Pr(d_1=5)} = 0$.

$\Pr(s = 5 | d_1 = 6) = \frac{\Pr(d_1=5 \wedge d_2=-1)}{\Pr(d_1=6)} = 0$.

The rest are similar. Many are 0.

Conditional Probability Example with a Biased Coin

Bill has two coins F (for Fair) and B (for Biased) $\Pr(H) = \frac{3}{4}$).
He picks one at random (using a sep fair coin).
He flips the coin.

Conditional Probability Example with a Biased Coin

Bill has two coins F (for Fair) and B (for Biased) $\Pr(H) = \frac{3}{4}$).
He picks one at random (using a sep fair coin).
He flips the coin.
$\Pr(H|B) = \frac{3}{4}$ by definition of Bias.
$\Pr(H|F) = \frac{1}{2}$ by definition of Fair.

Conditional Probability Example with a Biased Coin

Bill has two coins F (for Fair) and B (for Biased) $\Pr(H) = \frac{3}{4}$).
He picks one at random (using a sep fair coin).
He flips the coin.
$\Pr(H|B) = \frac{3}{4}$ by definition of Bias.
$\Pr(H|F) = \frac{1}{2}$ by definition of Fair.

$\Pr(B|H) = \frac{\Pr(B \cap H)}{\Pr(H)}$.

Conditional Probability Example with a Biased Coin

Bill has two coins F (for Fair) and B (for Biased) $\Pr(H) = \frac{3}{4}$).
He picks one at random (using a sep fair coin).
He flips the coin.
$\Pr(H|B) = \frac{3}{4}$ by definition of Bias.
$\Pr(H|F) = \frac{1}{2}$ by definition of Fair.

$\Pr(B|H) = \frac{\Pr(B \cap H)}{\Pr(H)}$.

$\Pr(B \cap H) = \Pr(B) \times \Pr(H|B) = \frac{1}{2} \times \frac{3}{4} = \frac{3}{8}$.
$\Pr(H) = \Pr(B) \times \Pr(H|B) + \Pr(F) \times \Pr(H|F) = \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{3}{4} = \frac{5}{8}$

Conditional Probability Example with a Biased Coin

Bill has two coins F (for Fair) and B (for Biased) $\Pr(H) = \frac{3}{4}$).
He picks one at random (using a sep fair coin).
He flips the coin.
$\Pr(H|B) = \frac{3}{4}$ by definition of Bias.
$\Pr(H|F) = \frac{1}{2}$ by definition of Fair.

$\Pr(B|H) = \frac{\Pr(B \cap H)}{\Pr(H)}$.

$\Pr(B \cap H) = \Pr(B) \times \Pr(H|B) = \frac{1}{2} \times \frac{3}{4} = \frac{3}{8}$.
$\Pr(H) = \Pr(B) \times \Pr(H|B) + \Pr(F) \times \Pr(H|F) = \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{3}{4} = \frac{5}{8}$

$\Pr(B|H) = \frac{\Pr(B \cap H)}{\Pr(H)} = \frac{3/8}{5/8} = \frac{3}{5}$.

Definition of a Secure Crypto System

m will be a message.

Definition of a Secure Crypto System

m will be a message. c is what is sent.
If the following holds then the system is **secure**.

$$(\forall m, x, y, c)[\Pr(m = x | c = y) = \Pr(m = x)].$$

So seeing the y does not help Eve **at all**.

Definition of a Secure Crypto System

m will be a message. c is what is sent.
If the following holds then the system is **secure**.

$$(\forall m, x, y, c)[\Pr(m = x | c = y) = \Pr(m = x)].$$

So seeing the y does not help Eve **at all**.
Is this info-theoretic security or comp-security? Discuss

Definition of a Secure Crypto System

m will be a message. c is what is sent.
If the following holds then the system is **secure**.

$$(\forall m, x, y, c)[\Pr(m = x | c = y) = \Pr(m = x)].$$

So seeing the y does not help Eve **at all**.
Is this info-theoretic security or comp-security? Discuss
Info-Theoretic If Eve has unlimited computing power she still learns **nothing**.

One-Letter Shift is Secure!

Alphabet is $\{x, y\}$. $s \in \{0, 1\}$ randomly.
$\Pr(m = x) = p_x$. $\Pr(m = y) = p_y$.

One-Letter Shift is Secure!

Alphabet is $\{x, y\}$. $s \in \{0, 1\}$ randomly.
$\Pr(m = x) = p_x$. $\Pr(m = y) = p_y$. Eve knows this.

One-Letter Shift is Secure!

Alphabet is $\{x, y\}$. $s \in \{0, 1\}$ randomly.
$\Pr(m = x) = p_x$. $\Pr(m = y) = p_y$. Eve knows this.
Note that $p_x + p_y = 1$.

One-Letter Shift is Secure!

Alphabet is $\{x, y\}$. $s \in \{0, 1\}$ randomly.
$\Pr(m = x) = p_x$. $\Pr(m = y) = p_y$. Eve knows this.
Note that $p_x + p_y = 1$.

$$\Pr(m = x | c = x) = \frac{\Pr(m = x \wedge c = x)}{\Pr(c = x)}$$

One-Letter Shift is Secure!

Alphabet is $\{x, y\}$. $s \in \{0, 1\}$ randomly.
$\Pr(m = x) = p_x$. $\Pr(m = y) = p_y$. Eve knows this.
Note that $p_x + p_y = 1$.

$$\Pr(m = x | c = x) = \frac{\Pr(m = x \wedge c = x)}{\Pr(c = x)}$$

$\Pr(m = x \wedge c = x) = \Pr(m = x \wedge s = 0) = p_x \times \frac{1}{2} = 0.5 p_x$

One-Letter Shift is Secure!

Alphabet is $\{x, y\}$. $s \in \{0, 1\}$ randomly.
$\mathrm{Pr}(m = x) = p_x$. $\mathrm{Pr}(m = y) = p_y$. Eve knows this.
Note that $p_x + p_y = 1$.

$$\mathrm{Pr}(m = x | c = x) = \frac{\mathrm{Pr}(m = x \wedge c = x)}{\mathrm{Pr}(c = x)}$$

$\mathrm{Pr}(m = x \wedge c = x) = \mathrm{Pr}(m = x \wedge s = 0) = p_x \times \frac{1}{2} = 0.5p_x$
$\mathrm{Pr}(c = x) = \mathrm{Pr}(m = x)\mathrm{Pr}(s = 0) + \mathrm{Pr}(m = y)\mathrm{Pr}(s = 1) =$
$0.5p_x + 0.5p_y = 0.5(p_x + p_y)$

One-Letter Shift is Secure!

Alphabet is $\{x, y\}$. $s \in \{0, 1\}$ randomly.
$\Pr(m = x) = p_x$. $\Pr(m = y) = p_y$. Eve knows this.
Note that $p_x + p_y = 1$.

$$\Pr(m = x | c = x) = \frac{\Pr(m = x \wedge c = x)}{\Pr(c = x)}$$

$\Pr(m = x \wedge c = x) = \Pr(m = x \wedge s = 0) = p_x \times \frac{1}{2} = 0.5p_x$
$\Pr(c = x) = \Pr(m = x)\Pr(s = 0) + \Pr(m = y)\Pr(s = 1) = 0.5p_x + 0.5p_y = 0.5(p_x + p_y)$

$$\Pr(m = x | c = x) = \frac{0.5p_x}{0.5(p_x + p_y)} = p_x$$

One-Letter Shift is Secure! (cont)

Alphabet is $\{x, y\}$. $s \in \{0, 1\}$ randomly.
$\Pr(m = x) = p_x$. $\Pr(m = y) = p_y$.

One-Letter Shift is Secure! (cont)

Alphabet is $\{x, y\}$. $s \in \{0, 1\}$ randomly.
$\Pr(m = x) = p_x$. $\Pr(m = y) = p_y$. Eve knows this.

One-Letter Shift is Secure! (cont)

Alphabet is $\{x, y\}$. $s \in \{0, 1\}$ randomly.
$\Pr(m = x) = p_x$. $\Pr(m = y) = p_y$. Eve knows this.
Note that $p_x + p_y = 1$.
We showed

$$\Pr(m = x | c = x) = p_x$$

One-Letter Shift is Secure! (cont)

Alphabet is $\{x, y\}$. $s \in \{0, 1\}$ randomly.
$\Pr(m = x) = p_x$. $\Pr(m = y) = p_y$. Eve knows this.
Note that $p_x + p_y = 1$.
We showed

$$\Pr(m = x|c = x) = p_x$$

One can show:

$$\Pr(m = x|c = y) = p_x.$$

$$\Pr(m = y|c = x) = p_y.$$

$$\Pr(m = y|c = y) = p_y.$$

One-Letter Shift is Secure! (cont)

Alphabet is $\{x, y\}$. $s \in \{0, 1\}$ randomly.
$\Pr(m = x) = p_x$. $\Pr(m = y) = p_y$. Eve knows this.
Note that $p_x + p_y = 1$.
We showed

$$\Pr(m = x | c = x) = p_x$$

One can show:

$$\Pr(m = x | c = y) = p_x.$$

$$\Pr(m = y | c = x) = p_y.$$

$$\Pr(m = y | c = y) = p_y.$$

So seeing the ciphertext gives Eve **NO INFORMATION**.
Upshot The 1-letter shift **Information-Theoretic Secure**.

Is 2-letter Shift Uncrackable?

Is 2-letter Shift Uncrackable? Discuss.

Is 2-letter Shift Uncrackable?

Is 2-letter Shift Uncrackable? Discuss.
No. Alphabet is $\{X, Y\}$.

Is 2-letter Shift Uncrackable?

Is 2-letter Shift Uncrackable? Discuss.
No. Alphabet is $\{X, Y\}$.
If Eve sees **XX** then she knows that the original message was one of

$$\{XX, YY\}$$

So Eve has learned something. HW will make this rigorous.

Summary and a New Question

Summary and a New Question

- Alice and Bob use shift s unif, 1-letter.

Summary and a New Question

- Alice and Bob use shift s unif, 1-letter. **Secure**

Summary and a New Question

- Alice and Bob use shift s unif, 1-letter. **Secure**
- Alice and Bob use shift s bias, 1-letter.

Summary and a New Question

- Alice and Bob use shift s unif, 1-letter. **Secure**
- Alice and Bob use shift s bias, 1-letter. **Insecure**

Summary and a New Question

- Alice and Bob use shift s unif, 1-letter. **Secure**
- Alice and Bob use shift s bias, 1-letter. **Insecure**
- Alice and Bob use shift s unif, 2-letters.

Summary and a New Question

- Alice and Bob use shift s unif, 1-letter. **Secure**
- Alice and Bob use shift s bias, 1-letter. **Insecure**
- Alice and Bob use shift s unif, 2-letters. **Insecure**

Summary and a New Question

- Alice and Bob use shift s unif, 1-letter. **Secure**
- Alice and Bob use shift s bias, 1-letter. **Insecure**
- Alice and Bob use shift s unif, 2-letters. **Insecure**

New Question Is the last item that important?

Summary and a New Question

- Alice and Bob use shift s unif, 1-letter. **Secure**
- Alice and Bob use shift s bias, 1-letter. **Insecure**
- Alice and Bob use shift s unif, 2-letters. **Insecure**

New Question Is the last item that important?
We are saying that Eve knows prob stuff, but does she really KNOW something?

Can Two 1-Letter Messages Leak Information?

Can Two 1-Letter Messages using the same shift Leak Information?

Can Two 1-Letter Messages Leak Information?

Can Two 1-Letter Messages using the same shift Leak Information?
Yes

Can Two 1-Letter Messages Leak Information?

Can Two 1-Letter Messages using the same shift Leak Information?
Yes

Scenario

Visible to all: **Is Eric a double agent working for the Klingons?**

Can Two 1-Letter Messages Leak Information?

Can Two 1-Letter Messages using the same shift Leak Information?
Yes

Scenario

Visible to all: **Is Eric a double agent working for the Klingons?**
The answer comes via a shift cipher: **A** (which is either Y or N)

Can Two 1-Letter Messages Leak Information?

Can Two 1-Letter Messages using the same shift Leak Information?
Yes

Scenario

Visible to all: **Is Eric a double agent working for the Klingons?**
The answer comes via a shift cipher: **A** (which is either Y or N)

In clear: **Is Eric a double agent working for the Romulans?**

Can Two 1-Letter Messages Leak Information?

Can Two 1-Letter Messages using the same shift Leak Information?
Yes

Scenario

Visible to all: **Is Eric a double agent working for the Klingons?**
The answer comes via a shift cipher: **A** (which is either Y or N)

In clear: **Is Eric a double agent working for the Romulans?**
The answer comes via a shift cipher: **A** (which is either Y or N)

Can Two 1-Letter Messages Leak Information?

Can Two 1-Letter Messages using the same shift Leak Information?
Yes

Scenario

Visible to all: **Is Eric a double agent working for the Klingons?**
The answer comes via a shift cipher: **A** (which is either Y or N)

In clear: **Is Eric a double agent working for the Romulans?**
The answer comes via a shift cipher: **A** (which is either Y or N)

Since the answer to both questions was **the same**, namely A,
Eve knows Eric is working for either **both** or **neither.**

Eve Can Tell if Two Message Are Same

Issue If Eve sees two messages, will know if they are the same or different.

Does this leak information Discuss.

Eve Can Tell if Two Message Are Same

Issue If Eve sees two messages, will know if they are the same or different.

Does this leak information Discuss. Yes.

Eve Can Tell if Two Message Are Same

Issue If Eve sees two messages, will know if they are the same or different.

Does this leak information Discuss. Yes.

What to do about this? Discuss.

Eve Can Tell if Two Message Are Same

Issue If Eve sees two messages, will know if they are the same or different.

Does this leak information Discuss. Yes.

What to do about this? Discuss.

For Now Nothing Will come back to this issue after a few more ciphers.

Eve Can Tell if Two Message Are Same

Issue If Eve sees two messages, will know if they are the same or different.

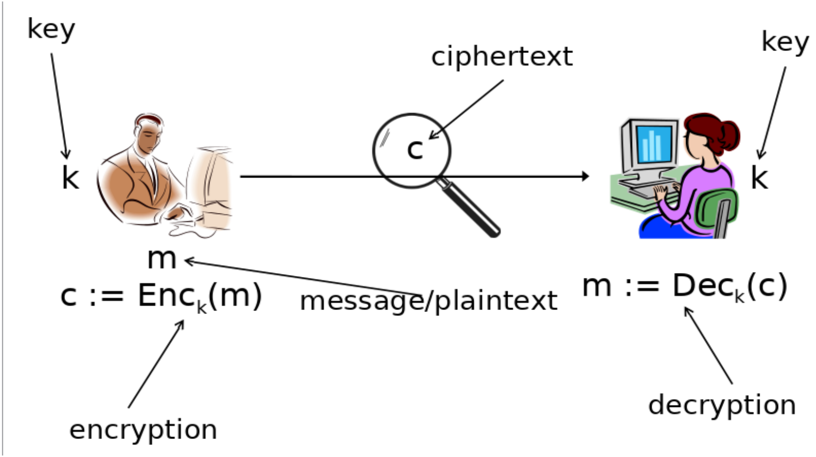
Does this leak information Discuss. Yes.

What to do about this? Discuss.

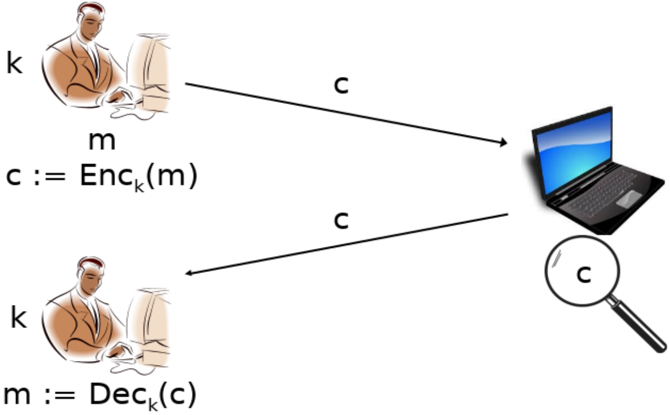
For Now Nothing Will come back to this issue after a few more ciphers.

For Now A lesson in how even defining **security** and **leak** must be done carefully.

Private-Key Encryption



Private-key encryption



Private-key encryption

- A *private-key encryption scheme* is defined by a message space $\mathcal{M}$ and algorithms **(Gen, Enc, Dec)**
  - **Gen** (key generation algorithm): outputs $k \in \mathcal{K}$
    (For SHIFT this is $k \in \{0, \ldots, 25\}$. Should 0 be included?)
  - **Enc** (encryption algorithm): takes key k and message $m \in \mathcal{M}$ as input; outputs ciphertext c
    $$c \leftarrow Enc_k(m)$$
    (For SHIFT this is $\text{Enc}(m_1, \ldots, m_n) = (m_1 + k, \ldots, m_n + k)$.)
  - **Dec** (decryption algorithm): takes key k and ciphertext c as input; outputs m or "error"
    $$m := Dec_k(c)$$
    (For SHIFT this is $\text{Dec}(c_1, \ldots, c_n) = (c_1 - k, \ldots, c_n - k)$.)
$$\forall k \text{ output by Gen } \forall m \in \mathcal{M}, Dec_k(Enc_k(m)) = m$$
(For SHIFT this is $(m + k) - k = m$)

BILL, STOP RECORDING LECTURE!!!!

BILL STOP RECORD LECTURE!!!