Cryptography

Lecture 2: Vigenère Cipher & Perfect Secrecy

October 23, 2026

Next Dates

Lecture (Fri 1:15pm)
Oct 23rd Lecture 2: Vigenère cipher & One-time pad
30th Lecture 3: Indistinguishability & Limits of Perfect Secrecy
Nov 6th Lecture 4: Pseudorandom Generators
13th Lecture 5: Multiple Encryptions
20th Lecture 6: Pseudorandom Functions
27th Lecture 7: Operation Modes
Dec 4th Lecture 8: Message Authentication Codes
11th Lecture 9: Authenticated Encryption

Lecture (Fri 1:15pm)
Dec 18th Lecture 10: Hash functions
25th —
Jan 1st —
8th Lecture 11: RSA & Diffie-Hellman assumptions
15th Lecture 12: Elliptic curves
22nd Lecture 13: Digital signatures
29th Lecture 14: Zero-Knowledge Proofs
Feb 5th Lecture 15: Reserve

Overview

Contents

1. Classical cryptography
   (Shift & Vigenère cipher, one-time pad, perfect secrecy)
2. Security definitions & threat models
   (Computational security, CPA & CCA)
3. Private-key cryptography
   (Message authentication, hash functions, primitives, relevant ciphers)
4. Public-key cryptography
   (Assumptions, key management, digital signatures, relevant ciphers)

Recall

Definition (§1.1 Simplistic encryption scheme)

Simplistic (private-key) encryption scheme for key space K is tuple

$$(M, C, \text{enc}, \text{dec})$$

- M and C are sets (message and ciphertext space)
- $\text{enc}\colon K \times M \to C$ and $\text{dec}\colon K \times C \to M$

Recall

Definition (§1.1 Simplistic encryption scheme)

Simplistic (private-key) encryption scheme for key space K is tuple

$$(M, C, \mathrm{enc}, \mathrm{dec})$$

- M and C are sets (message and ciphertext space)
- $\mathrm{enc}\colon K \times M \to C$ and $\mathrm{dec}\colon K \times C \to M$
- $\mathrm{dec}_k(\mathrm{enc}_k(m)) = m$ for all $k \in K$ and $m \in M$ (correctness)

Recall

Definition (§1.1 Simplistic encryption scheme)

Simplistic (private-key) encryption scheme for key space K is tuple

$$(M, C, \mathrm{enc}, \mathrm{dec})$$

- M and C are sets (message and ciphertext space)
- $\mathrm{enc}\colon K \times M \to C$ and $\mathrm{dec}\colon K \times C \to M$
- $\mathrm{dec}_k(\mathrm{enc}_k(m)) = m$ for all $k \in K$ and $m \in M$ (correctness)

Principles

- Scheme is not secret — Kerckhoffs
- Key space sufficiently large

Monoalphabetic Cipher

§2.1 Example (Monoalphabetic cipher)

- Key space $K = \{b \colon \Sigma \to \Sigma \mid b \text{ bijective}\}$ with $\Sigma = \{\text{'a'}, \text{'b'}, \ldots, \text{'z'}\}$
- Message space $M = \Sigma^*$
- Ciphertext space $C = \Sigma^*$
- Encryption $\mathrm{enc}_b(m_1, \ldots, m_n) = \big(b(m_1), \ldots, b(m_n)\big)$
- Decryption $\mathrm{dec}_b(c_1, \ldots, c_n) = \big(b^{-1}(c_1), \ldots, b_n^{-1}(c_n)\big)$

Monoalphabetic Cipher

§2.1 Example (Monoalphabetic cipher)

- Key space $K = \{b \colon \Sigma \to \Sigma \mid b \text{ bijective}\}$ with $\Sigma = \{\text{'a'}, \text{'b'}, \ldots, \text{'z'}\}$
- Message space $M = \Sigma^*$
- Ciphertext space $C = \Sigma^*$
- Encryption $\text{enc}_b(m_1, \ldots, m_n) = \big(b(m_1), \ldots, b(m_n)\big)$
- Decryption $\text{dec}_b(c_1, \ldots, c_n) = \big(b^{-1}(c_1), \ldots, b_n^{-1}(c_n)\big)$

Note

- Caesar & shift cipher are monoalphabetic

Monoalphabetic Cipher

§2.1 Example (Monoalphabetic cipher)

- Key space $K = \{b \colon \Sigma \to \Sigma \mid b \text{ bijective}\}$ with $\Sigma = \{\text{'a'}, \text{'b'}, \ldots, \text{'z'}\}$
- Message space $M = \Sigma^*$
- Ciphertext space $C = \Sigma^*$
- Encryption $\text{enc}_b(m_1, \ldots, m_n) = (b(m_1), \ldots, b(m_n))$
- Decryption $\text{dec}_b(c_1, \ldots, c_n) = (b^{-1}(c_1), \ldots, b_n^{-1}(c_n))$

Note

- Caesar & shift cipher are monoalphabetic

Illustration of bijection b

σ	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
$b(\sigma)$	k	d	g	f	n	s	l	v	b	w	a	h	e	x	j	m	q	c	p	z	r	t	y	i	u	o

Monoalphabetic Cipher

Key (bijection) b

σ	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
$b(\sigma)$	k	d	g	f	n	s	l	v	b	w	a	h	e	x	j	m	q	c	p	z	r	t	y	i	u	o

Monoalphabetic Cipher

Key (bijection) b

σ	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
$b(\sigma)$	k	d	g	f	n	s	l	v	b	w	a	h	e	x	j	m	q	c	p	z	r	t	y	i	u	o

Illustration

- Ciphertext $\mathrm{enc}_b(\text{“hello”}) = \text{“vnhhj”}$

Monoalphabetic Cipher

Key (bijection) b

σ	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
$b(\sigma)$	k	d	g	f	n	s	l	v	b	w	a	h	e	x	j	m	q	c	p	z	r	t	y	i	u	o

Illustration

- Ciphertext $\mathrm{enc}_b(\text{“hello”}) = \text{“vnhhj”}$
- Message $\mathrm{dec}_b(\text{“vnhhj”}) = \text{“hello”}$

Monoalphabetic Cipher

Size of key space

$$26! = 4.03 \cdot 10^{26} \geq 2^{88}$$

Monoalphabetic Cipher

Size of key space

$$26! = 4.03 \cdot 10^{26} \geq 2^{88}$$

Sufficiently large key space

- Suppose decrypt/analysis takes 1 as per key candidate

  (1,000 AMD Threadripper 7980X [64,000 cores]: $6.8 \cdot 10^9$ MIPS)

  (Fujitsu Fugaku [7,630,848 cores]: $537 \cdot 10^9$ MIPS)

  (HPE Frontier [591,872 cores]: $1,686 \cdot 10^9$ MIPS)

  ($\rightarrow$ AMD: 6.8 instructions per fs Frontier: 1.686 instructions per as)

- Brute-force attack takes $4.03 \cdot 10^8$ s $\approx$ 12.8 years

Monoalphabetic Cipher

Size of key space

$$26! = 4.03 \cdot 10^{26} \geq 2^{88}$$

Sufficiently large key space

- Suppose decrypt/analysis takes 1 as per key candidate

  (1,000 AMD Threadripper 7980X [64,000 cores]: $6.8 \cdot 10^9$ MIPS)

  (Fujitsu Fugaku [7,630,848 cores]: $537 \cdot 10^9$ MIPS)

  (HPE Frontier [591,872 cores]: $1,686 \cdot 10^9$ MIPS)

  ($\rightarrow$ AMD: 6.8 instructions per fs Frontier: 1.686 instructions per as)

- Brute-force attack takes $4.03 \cdot 10^8$ s $\approx$ 12.8 years

So is this scheme secure?

Monoalphabetic Cipher

All monoalphabetic ciphers are insecure

Monoalphabetic Cipher

All monoalphabetic ciphers are insecure

Attacks

- Shift-cipher attack fails in general
- Frequency analysis still successful (→ exercise)

Vigenère Cipher

§2.2 Example (Vigenère cipher; actually Giovan Battista Bellaso 1553)

- Key space $K = \Sigma^+$ with $\Sigma = \{\text{'a'}, \text{'b'}, \ldots, \text{'z'}\}$
- Message and ciphertext space $M = C = \Sigma^*$
- Encryption $\mathrm{enc}_k(m_1, \ldots, m_n) = (m_1 \oplus k_{0 \bmod \ell}, \ldots, m_n \oplus k_{(n-1) \bmod \ell})$ with key $k = (k_0, \ldots, k_{\ell-1})$
- Decryption $\mathrm{dec}_k(c_1, \ldots, c_n) = (c_1 \ominus k_{0 \bmod \ell}, \ldots, c_n \ominus k_{(n-1) \bmod \ell})$

Blaise de Vigenère (* 1523; † 1596)

- French diplomat, cryptographer & alchemist
- Diplomatic mission to Rome
- Vigenère cipher misattributed in 19th century; he developed stronger autokey cipher



Vigenère Cipher

Notes

- $\oplus$ and $\ominus$ modular arithmetic on letters according to alphabet position
- Considered unbreakable until 1863 (Kasiski attack)

Vigenère Cipher

Notes

- $\oplus$ and $\ominus$ modular arithmetic on letters according to alphabet position
- Considered unbreakable until 1863 (Kasiski attack)

Illustration

message	t	h	i	s	i	s	t	h	e	s	e	c	r	e	t	m	e	s	s	a	g	e
repeated key	p	a	r	t	y	p	a	r	t	y	p	a	r	t	y	p	a	r	t	y	p	a
ciphertext	i	h	z	l	g	h	t	y	x	q	t	c	i	x	r	b	e	j	l	y	v	e

Vigenère Cipher

Notes

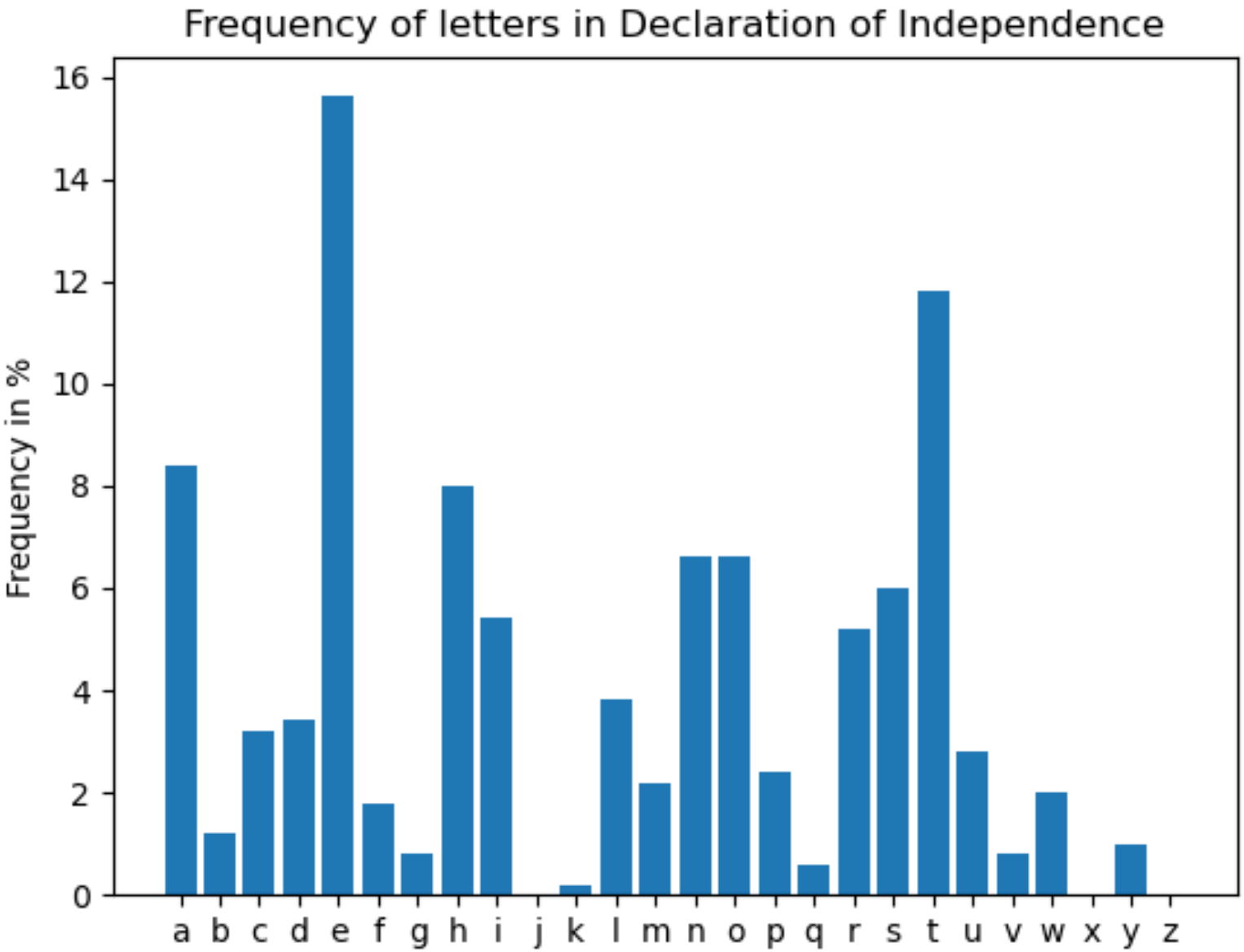
- $\oplus$ and $\ominus$ modular arithmetic on letters according to alphabet position
- Considered unbreakable until 1863 (Kasiski attack)

Illustration

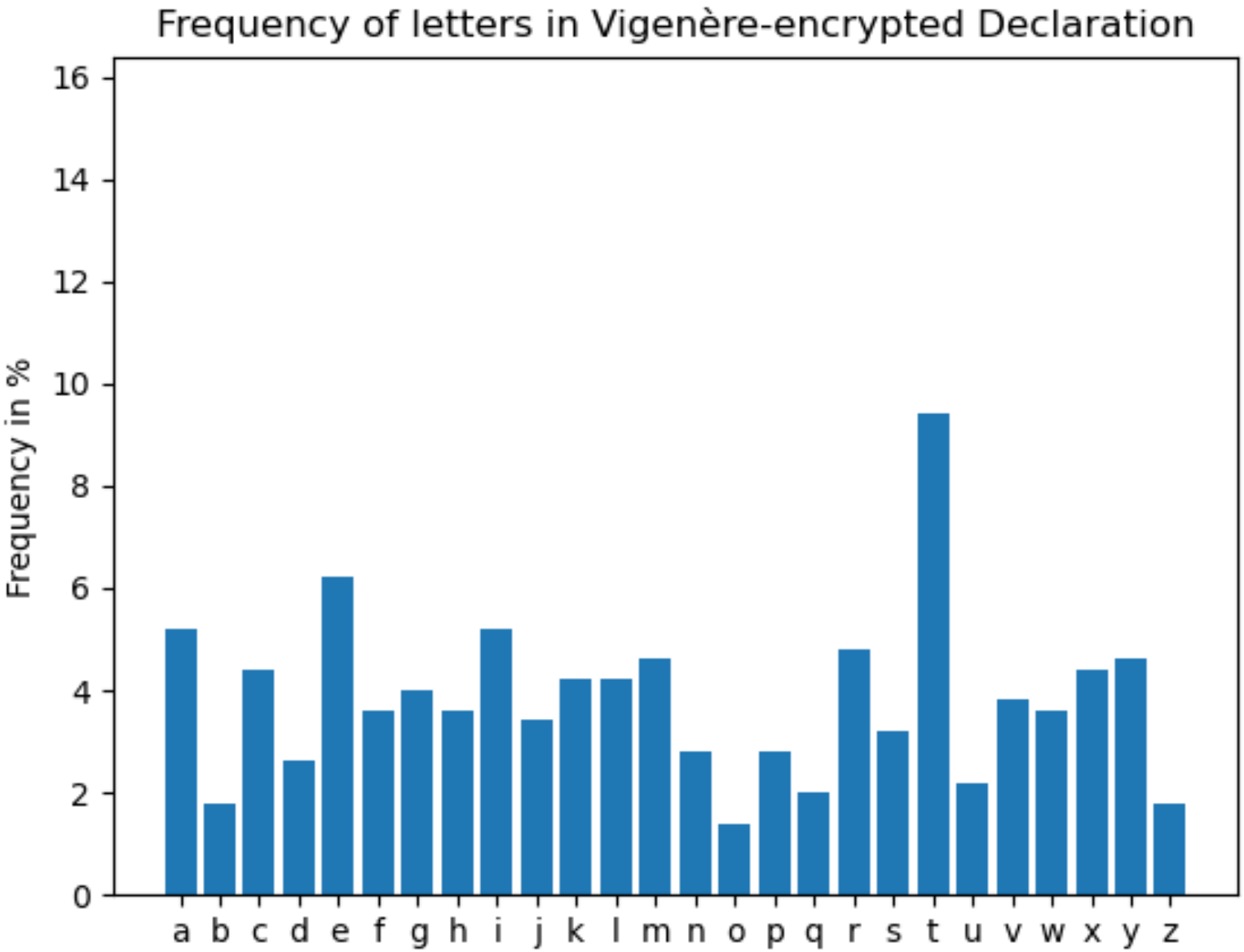
message	t	h	i	s	i	s	t	h	e	s	e	c	r	e	t	m	e	s	s	a	g	e
repeated key	p	a	r	t	y	p	a	r	t	y	p	a	r	t	y	p	a	r	t	y	p	a
ciphertext	i	h	z	l	g	h	t	y	x	q	t	c	i	x	r	b	e	j	l	y	v	e

- Sample computation 't' $\oplus$ 'p' = 'i' $\qquad 19 + 15 \bmod 26 = 8$

Cryptanalysis of Vigenère Cipher



Cryptanalysis of Vigenère Cipher



Cryptanalysis of Vigenère Cipher

Main insights

- No monoalphabetic cipher (unless key length 1)

Cryptanalysis of Vigenère Cipher

Main insights

- No monoalphabetic cipher (unless key length 1)
- Suppose key length $|k| = \ell$ and cipher text $c = c_1 \cdots c_n$

Cryptanalysis of Vigenère Cipher

Main insights

- No monoalphabetic cipher (unless key length 1)
- Suppose key length $|k| = \ell$ and cipher text $c = c_1 \cdots c_n$
  - $w_i^{(\ell)} = c_{i+0\ell} c_{i+1\ell} c_{i+2\ell} \cdots$ encrypted by shift k_{i-1} for all $1 \leq i \leq \ell$

Cryptanalysis of Vigenère Cipher

Main insights

- No monoalphabetic cipher (unless key length 1)
- Suppose key length $|k| = \ell$ and cipher text $c = c_1 \cdots c_n$
  - $w_i^{(\ell)} = c_{i+0\ell} c_{i+1\ell} c_{i+2\ell} \cdots$ encrypted by shift k_{i-1} for all $1 \leq i \leq \ell$
  - Provided c is long enough $\rightarrow$ $w_i^{(\ell)}$ long enough

Cryptanalysis of Vigenère Cipher

Main insights

- No monoalphabetic cipher (unless key length 1)
- Suppose key length $|k| = \ell$ and cipher text $c = c_1 \cdots c_n$
  - $w_i^{(\ell)} = c_{i+0\ell} c_{i+1\ell} c_{i+2\ell} \cdots$ encrypted by shift k_{i-1} for all $1 \leq i \leq \ell$
  - Provided c is long enough $\rightarrow$ $w_i^{(\ell)}$ long enough
  - Break shift cipher on $w_i^{(\ell)}$ to determine k_{i-1}

Cryptanalysis of Vigenère Cipher

Main insights

- No monoalphabetic cipher (unless key length 1)
- Suppose key length $|k| = \ell$ and cipher text $c = c_1 \cdots c_n$
  - $w_i^{(\ell)} = c_{i+0\ell} c_{i+1\ell} c_{i+2\ell} \cdots$ encrypted by shift k_{i-1} for all $1 \leq i \leq \ell$
  - Provided c is long enough $\rightarrow$ $w_i^{(\ell)}$ long enough
  - Break shift cipher on $w_i^{(\ell)}$ to determine k_{i-1}
  - Determine all key letters $k = k_0 \cdots k_{\ell-1}$

Cryptanalysis of Vigenère Cipher

Main insights

- No monoalphabetic cipher (unless key length 1)
- Suppose key length $|k| = \ell$ and cipher text $c = c_1 \cdots c_n$
  - $w_i^{(\ell)} = c_{i+0\ell}\, c_{i+1\ell}\, c_{i+2\ell} \cdots$ encrypted by shift k_{i-1} for all $1 \leq i \leq \ell$
  - Provided c is long enough $\rightarrow$ $w_i^{(\ell)}$ long enough
  - Break shift cipher on $w_i^{(\ell)}$ to determine k_{i-1}
  - Determine all key letters $k = k_0 \cdots k_{\ell-1}$

Illustration

message	t	h	i	s	i	s	t	h	e	s	e	c	r	e	t	m	e	s	s	a	g	e
repeated key	p	a	r	t	y	p	a	r	t	y	p	a	r	t	y	p	a	r	t	y	p	a
ciphertext	i	h	z	l	g	h	t	y	x	q	t	c	i	x	r	b	e	j	l	y	v	e

Cryptanalysis of Vigenère Cipher

Main insights

- No monoalphabetic cipher (unless key length 1)
- Suppose key length $|k| = \ell$ and cipher text $c = c_1 \cdots c_n$
  - $w_i^{(\ell)} = c_{i+0\ell}\, c_{i+1\ell}\, c_{i+2\ell} \cdots$ encrypted by shift k_{i-1} for all $1 \leq i \leq \ell$
  - Provided c is long enough $\rightarrow$ $w_i^{(\ell)}$ long enough
  - Break shift cipher on $w_i^{(\ell)}$ to determine k_{i-1}
  - Determine all key letters $k = k_0 \cdots k_{\ell-1}$

Illustration

message	t	h	i	s	i	s	t	h	e	s	e	c	r	e	t	m	e	s	s	a	g	e
repeated key	p	a	r	t	y	p	a	r	t	y	p	a	r	t	y	p	a	r	t	y	p	a
ciphertext	i	h	z	l	g	h	t	y	x	q	t	c	i	x	r	b	e	j	l	y	v	e

Cryptanalysis of Vigenère Cipher

Main insights

- No monoalphabetic cipher (unless key length 1)
- Suppose key length $|k| = \ell$ and cipher text $c = c_1 \cdots c_n$
  - $w_i^{(\ell)} = c_{i+0\ell}\, c_{i+1\ell}\, c_{i+2\ell} \cdots$ encrypted by shift k_{i-1} for all $1 \leq i \leq \ell$
  - Provided c is long enough $\rightarrow$ $w_i^{(\ell)}$ long enough
  - Break shift cipher on $w_i^{(\ell)}$ to determine k_{i-1}
  - Determine all key letters $k = k_0 \cdots k_{\ell-1}$

Illustration

message	t	h	i	s	i	s	t	h	e	s	e	c	r	e	t	m	e	s	s	a	g	e
repeated key	p	a	r	t	y	p	a	r	t	y	p	a	r	t	y	p	a	r	t	y	p	a
ciphertext	i	h	z	l	g	h	t	y	x	q	t	c	i	x	r	b	e	j	l	y	v	e

Cryptanalysis of Vigenère Cipher

Main insights

- No monoalphabetic cipher (unless key length 1)
- Suppose key length $|k| = \ell$ and cipher text $c = c_1 \cdots c_n$
  - $w_i^{(\ell)} = c_{i+0\ell} c_{i+1\ell} c_{i+2\ell} \cdots$ encrypted by shift k_{i-1} for all $1 \leq i \leq \ell$
  - Provided c is long enough $\rightarrow$ $w_i^{(\ell)}$ long enough
  - Break shift cipher on $w_i^{(\ell)}$ to determine k_{i-1}
  - Determine all key letters $k = k_0 \cdots k_{\ell-1}$

Illustration

message	t	h	i	s	i	s	t	h	e	s	e	c	r	e	t	m	e	s	s	a	g	e
repeated key	p	a	r	t	y	p	a	r	t	y	p	a	r	t	y	p	a	r	t	y	p	a
ciphertext	i	h	z	l	g	h	t	y	x	q	t	c	i	x	r	b	e	j	l	y	v	e

How to determine key length?

Cryptanalysis of Vigenère Cipher

Determine key length

- Guess upper bound $\hat{\ell}$ on key length

Cryptanalysis of Vigenère Cipher

Determine key length

- Guess upper bound $\hat{\ell}$ on key length
- Determine $w_i^{(\ell)}$ for all $1 \leq \ell \leq \hat{\ell}$ and $1 \leq i \leq \ell$

Cryptanalysis of Vigenère Cipher

Determine key length

- Guess upper bound $\hat{\ell}$ on key length
- Determine $w_i^{(\ell)}$ for all $1 \leq \ell \leq \hat{\ell}$ and $1 \leq i \leq \ell$
- Perform frequency analysis on $w_i^{(\ell)}$; i.e. determine $I(w_i^{(\ell)})$

Cryptanalysis of Vigenère Cipher

Determine key length

- Guess upper bound $\hat{\ell}$ on key length
- Determine $w_i^{(\ell)}$ for all $1 \leq \ell \leq \hat{\ell}$ and $1 \leq i \leq \ell$
- Perform frequency analysis on $w_i^{(\ell)}$; i.e. determine $I(w_i^{(\ell)})$
- Select smallest i' such that $I(w_i^{(i')}) \approx I = 1.706926$ for all $1 \leq i \leq i'$

Cryptanalysis of Vigenère Cipher

Determine key length

- Guess upper bound $\hat{\ell}$ on key length
- Determine $w_i^{(\ell)}$ for all $1 \leq \ell \leq \hat{\ell}$ and $1 \leq i \leq \ell$
- Perform frequency analysis on $w_i^{(\ell)}$; i.e. determine $I(w_i^{(\ell)})$
- Select smallest i' such that $I(w_i^{(i')}) \approx I = 1.706926$ for all $1 \leq i \leq i'$
- Suppose key length is i' and proceed to break i' shift ciphers

Cryptanalysis of Vigenère Cipher

Determine key length

- Guess upper bound $\hat{\ell}$ on key length
- Determine $w_i^{(\ell)}$ for all $1 \leq \ell \leq \hat{\ell}$ and $1 \leq i \leq \ell$
- Perform frequency analysis on $w_i^{(\ell)}$; i.e. determine $I(w_i^{(\ell)})$
- Select smallest i' such that $I(w_i^{(i')}) \approx I = 1.706926$ for all $1 \leq i \leq i'$
- Suppose key length is i' and proceed to break i' shift ciphers

Questions

- Why does this work?
- Why smallest i' and not "best" (best-match) i'?
- What is expected value $I(w_i^{(i')})$ for wrong choice of i'?

Cryptanalysis of Vigenère Cipher

Letter counts b_i^m of message m with $n = |m|$

$$I(m) = 26 \sum_{i=0}^{25} \frac{b_i^m (b_i^m - 1)}{n(n-1)}$$

Cryptanalysis of Vigenère Cipher

Letter counts b_i^m of message m with $n = |m|$

$$I(m) = 26 \sum_{i=0}^{25} \frac{b_i^m (b_i^m - 1)}{n(n-1)}$$

$I(c_i^{(\ell)})$	$i=1$	$i=2$	$i=3$	$i=4$	$i=5$	$i=6$
$\ell=1$	1.128					
$\ell=2$	1.119	1.109				
$\ell=3$	1.047	1.240	1.105			
$\ell=4$	1.188	1.047	1.060	1.091		
$\ell=5$	2.017	2.064	1.917	1.943	1.629	
$\ell=6$	1.059	1.352	1.276	0.955	1.154	1.054

Cryptanalysis of Vigenère Cipher

Letter counts b_i^m of message m with $n = |m|$

$$I(m) = 26 \sum_{i=0}^{25} \frac{b_i^m (b_i^m - 1)}{n(n-1)}$$

$I(c_i^{(\ell)})$	$i=1$	$i=2$	$i=3$	$i=4$	$i=5$	$i=6$
$\ell=1$	1.128					
$\ell=2$	1.119	1.109				
$\ell=3$	1.047	1.240	1.105			
$\ell=4$	1.188	1.047	1.060	1.091		
$\ell=5$	2.017	2.064	1.917	1.943	1.629	
$\ell=6$	1.059	1.352	1.276	0.955	1.154	1.054

$\rightarrow$ Key length probably 5

Outlook

- Multiple additional ciphers & attacks (autokey ciphers, Enigma, etc.)

Outlook

- Multiple additional ciphers & attacks (autokey ciphers, Enigma, etc.)
- Classical cryptography was art
  - Ciphers developed & deployed (kept secret)
  - Tested only by initiated few

Outlook

- Multiple additional ciphers & attacks (autokey ciphers, Enigma, etc.)
- Classical cryptography was art
  - Ciphers developed & deployed (kept secret)
  - Tested only by initiated few
  - Eventually reverse-engineered & vulnerabilities discovered (often grave consequences; e.g. Enigma)
  - Cipher adjusted to prevent existing attacks (rinse & repeat)

Classic Ciphers

Outlook

- Multiple additional ciphers & attacks (autokey ciphers, Enigma, etc.)
- Classical cryptography was art
  - Ciphers developed & deployed (kept secret)
  - Tested only by initiated few
  - Eventually reverse-engineered & vulnerabilities discovered (often grave consequences; e.g. Enigma)
  - Cipher adjusted to prevent existing attacks (rinse & repeat)
- Perfect secrecy & one-time pad

Perfectly Secret Encryption

§2.3 Definition (Probabilistic algorithm)

Probabilistic algorithm is multi-tape deterministic Turing machine (DTM) that additionally has access to infinite read-only tape of (truly) random bits

Perfectly Secret Encryption

§2.3 Definition (Probabilistic algorithm)

Probabilistic algorithm is multi-tape deterministic Turing machine (DTM) that additionally has access to infinite read-only tape of (truly) random bits

Notes

- Compute computable probabilistic functions $f : \{0,1\}^\omega \times \Sigma^* \to \Delta^*$ for alphabets Σ and Δ with access to uniformly random bits $r \in \{0,1\}^\omega$
- We use $f_r : \Sigma^* \to \Delta^*$ when random bits r are known (rarely so)

Perfectly Secret Encryption

§2.3 Definition (Probabilistic algorithm)

Probabilistic algorithm is multi-tape deterministic Turing machine (DTM) that additionally has access to infinite read-only tape of (truly) random bits

Notes

- Compute computable probabilistic functions $f : \{0,1\}^\omega \times \Sigma^* \to \Delta^*$ for alphabets Σ and Δ with access to uniformly random bits $r \in \{0,1\}^\omega$
- We use $f_r : \Sigma^* \to \Delta^*$ when random bits r are known (rarely so)
- $f_r(x)$ essentially computable sampler from distribution over Δ^* (returns $f_r(x)$ based on random r)
- We use $\mathrm{P}\big[w \leftarrow f(x)\big]$ for $\mathrm{P}\big(\{r \mid f_r(x) = w\}\big)$ i.e. probability that $f_r(x)$ with uniformly random r returns w

Perfectly Secret Encryption

§2.3 Definition (Probabilistic algorithm)

Probabilistic algorithm is multi-tape deterministic Turing machine (DTM) that additionally has access to infinite read-only tape of (truly) random bits

Notes

- Compute computable probabilistic functions $f : \{0,1\}^\omega \times \Sigma^* \to \Delta^*$ for alphabets Σ and Δ with access to uniformly random bits $r \in \{0,1\}^\omega$
- We use $f_r : \Sigma^* \to \Delta^*$ when random bits r are known (rarely so)
- $f_r(x)$ essentially computable sampler from distribution over Δ^* (returns $f_r(x)$ based on random r)
- We use $\mathrm{P}\big[w \leftarrow f(x)\big]$ for $\mathrm{P}\big(\{r \mid f_r(x) = w\}\big)$ i.e. probability that $f_r(x)$ with uniformly random r returns w
- Sources of true randomness discussed later

Perfectly Secret Encryption

Additional notes & simplifications

- Modern notions & definitions (slightly overkill at this point)

Perfectly Secret Encryption

Additional notes & simplifications

- Modern notions & definitions (slightly overkill at this point)
- Random sequences $R = \{0,1\}^\omega$
- Message space $\emptyset \subsetneq M \subseteq \{0,1\}^*$

Perfectly Secret Encryption

Additional notes & simplifications

- Modern notions & definitions (slightly overkill at this point)
- Random sequences $R = \{0,1\}^\omega$
- Message space $\emptyset \subsetneq M \subseteq \{0,1\}^*$
- Key space $\emptyset \subsetneq K \subseteq \{0,1\}^*$
- Ciphertext space $\emptyset \subsetneq C \subseteq \{0,1\}^*$
- Messages, keys & ciphertexts coded in binary

Perfectly Secret Encryption

§2.4 Definition (Private-key encryption scheme)

Private-key encryption scheme is triple (gen, enc, dec)
of computable probabilistic functions

- gen: $R \to K$ yielding distribution $P_K: K \to [0,1]$
- enc: $R \times K \times M \to C$ and dec: $R \times K \times C \to M$

Perfectly Secret Encryption

§2.4 Definition (Private-key encryption scheme)

Private-key encryption scheme is triple $(\mathrm{gen}, \mathrm{enc}, \mathrm{dec})$ of computable probabilistic functions

- $\mathrm{gen}\colon R \to K$ yielding distribution $\mathrm{P}_K\colon K \to [0,1]$
- $\mathrm{enc}\colon R \times K \times M \to C$ and $\mathrm{dec}\colon R \times K \times C \to M$
- $\mathrm{dec}(r,k,c) = m$ for all $r \in R$, $k \in \mathrm{ran}(\mathrm{gen})$, $m \in M$, and $c \in C$ with $\mathrm{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] \neq 0$ (perfect correctness)

Perfectly Secret Encryption

§2.4 Definition (Private-key encryption scheme)

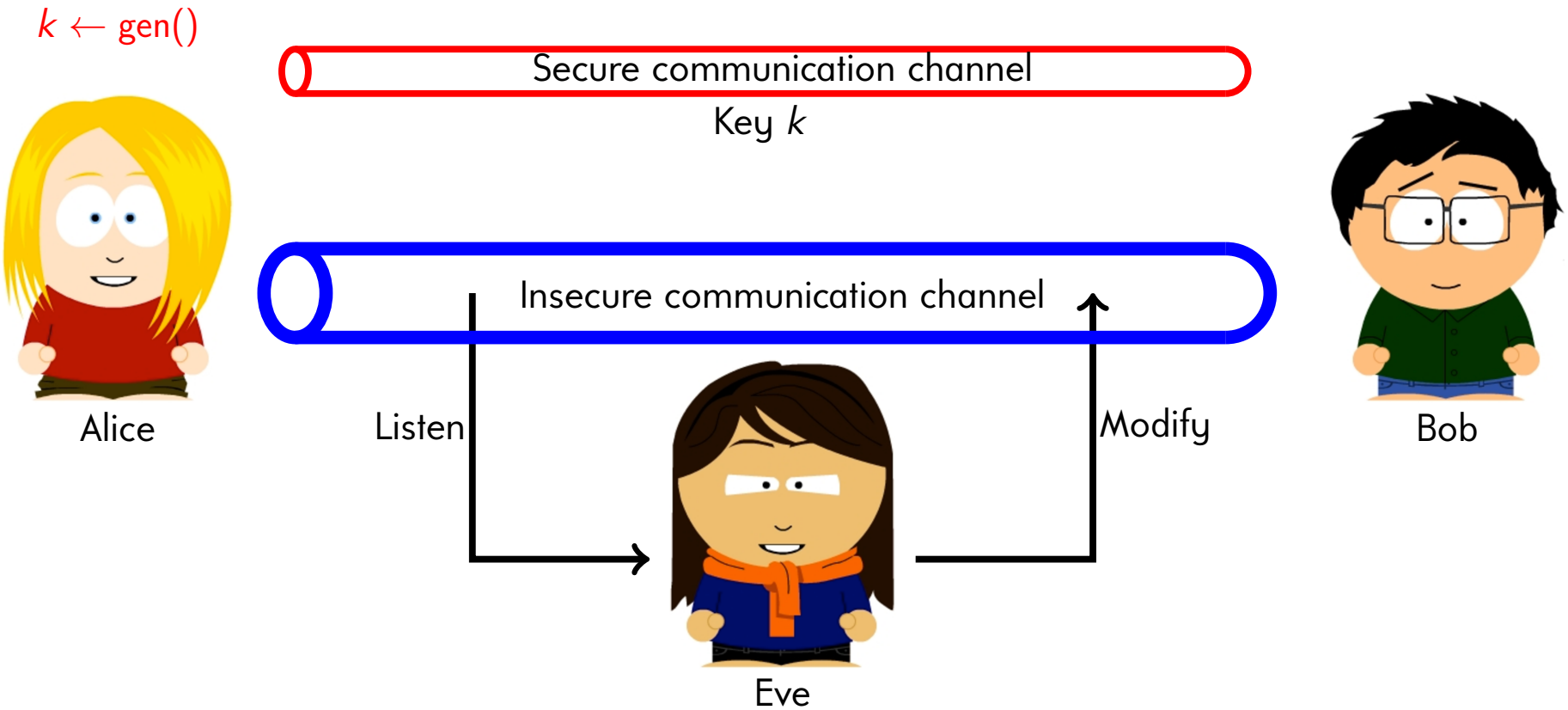
Private-key encryption scheme is triple $(\mathrm{gen}, \mathrm{enc}, \mathrm{dec})$ of computable probabilistic functions

- $\mathrm{gen}\colon R \to K$ yielding distribution $\mathrm{P}_K\colon K \to [0,1]$
- $\mathrm{enc}\colon R \times K \times M \to C$ and $\mathrm{dec}\colon R \times K \times C \to M$
- $\mathrm{dec}(r,k,c) = m$ for all $r \in R$, $k \in \mathrm{ran}(\mathrm{gen})$, $m \in M$, and $c \in C$ with $\mathrm{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] \neq 0$ (perfect correctness)

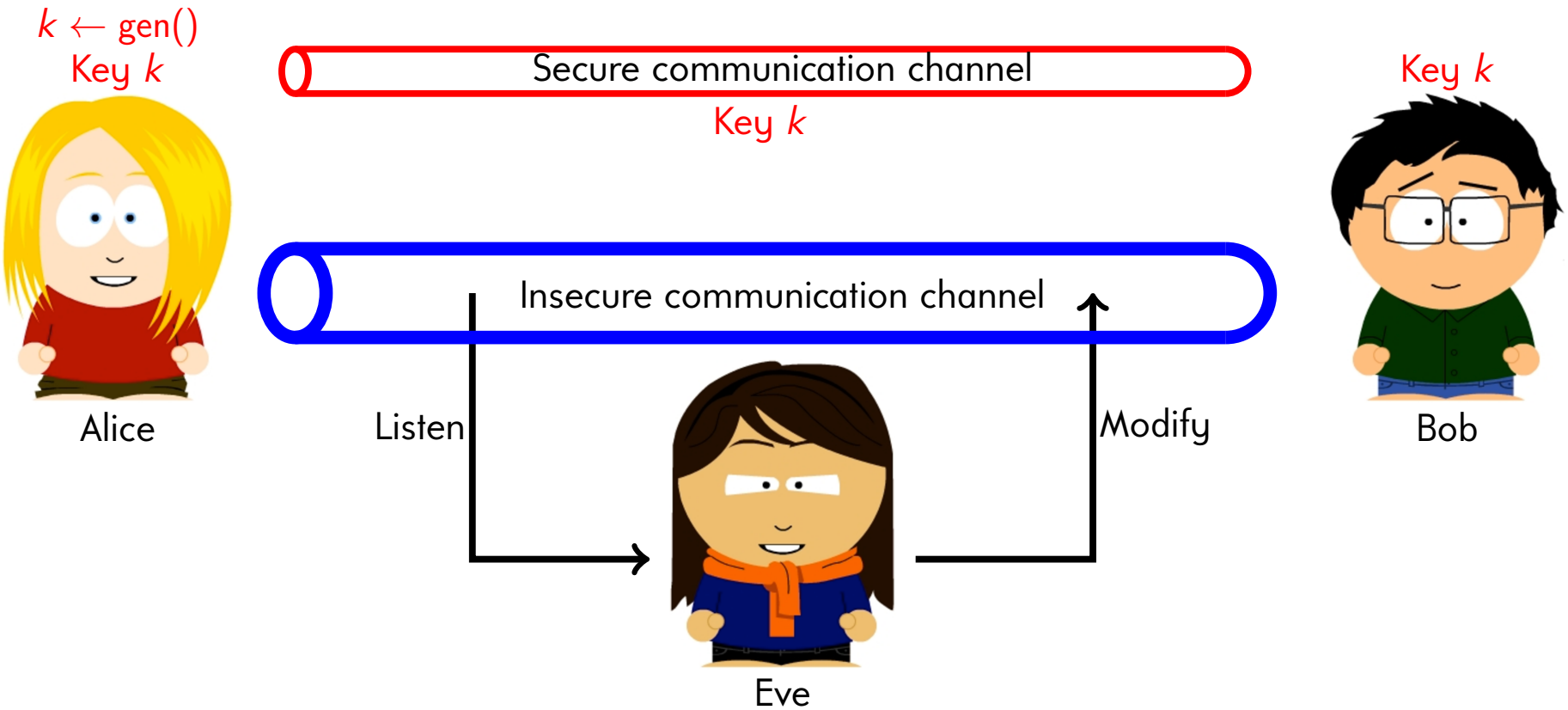
Notes

- Wlog. dec is not probabilistic, so $\mathrm{dec}\colon K \times C \to M$
- Scheme contains no distribution over messages
  (scheme is generic, i.e. agnostic to message distribution)

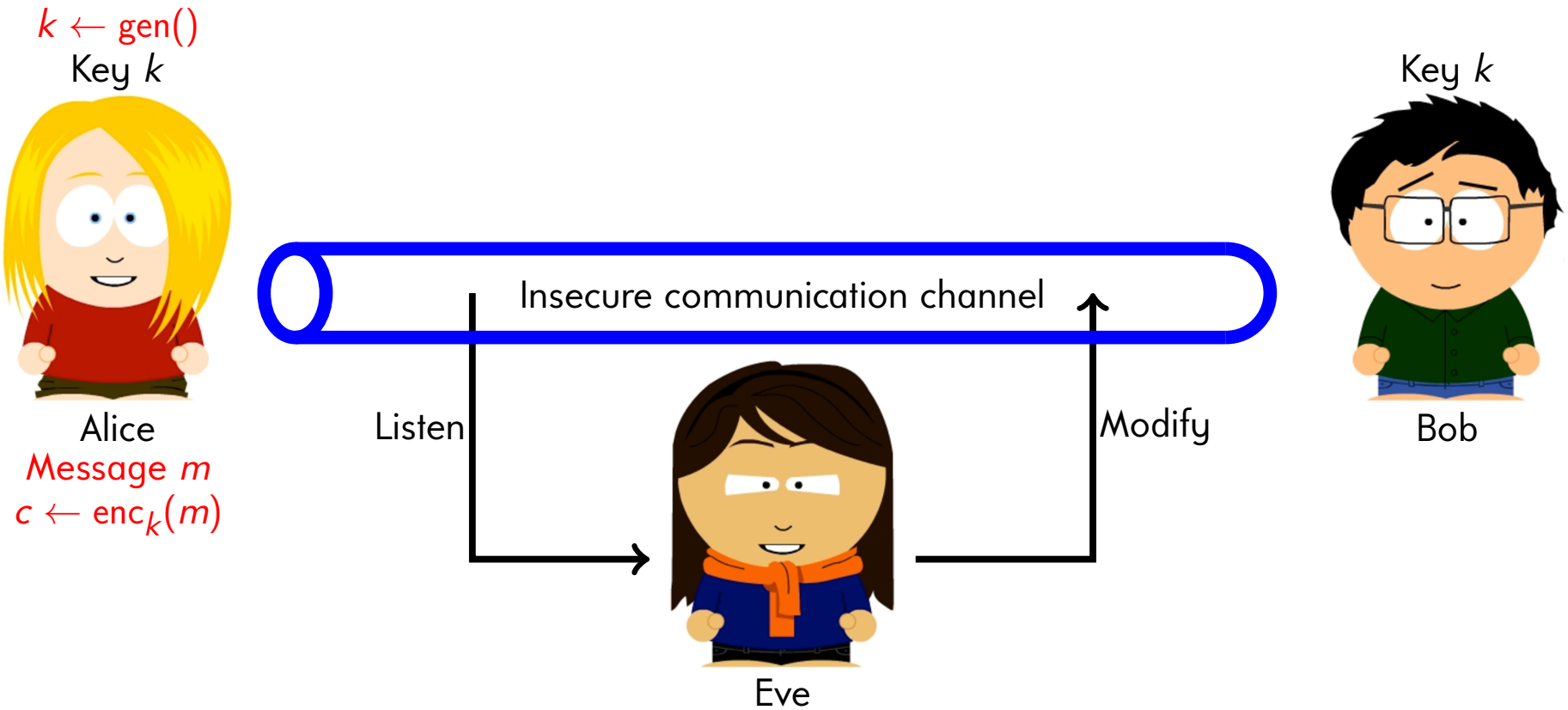
Perfectly Secret Encryption



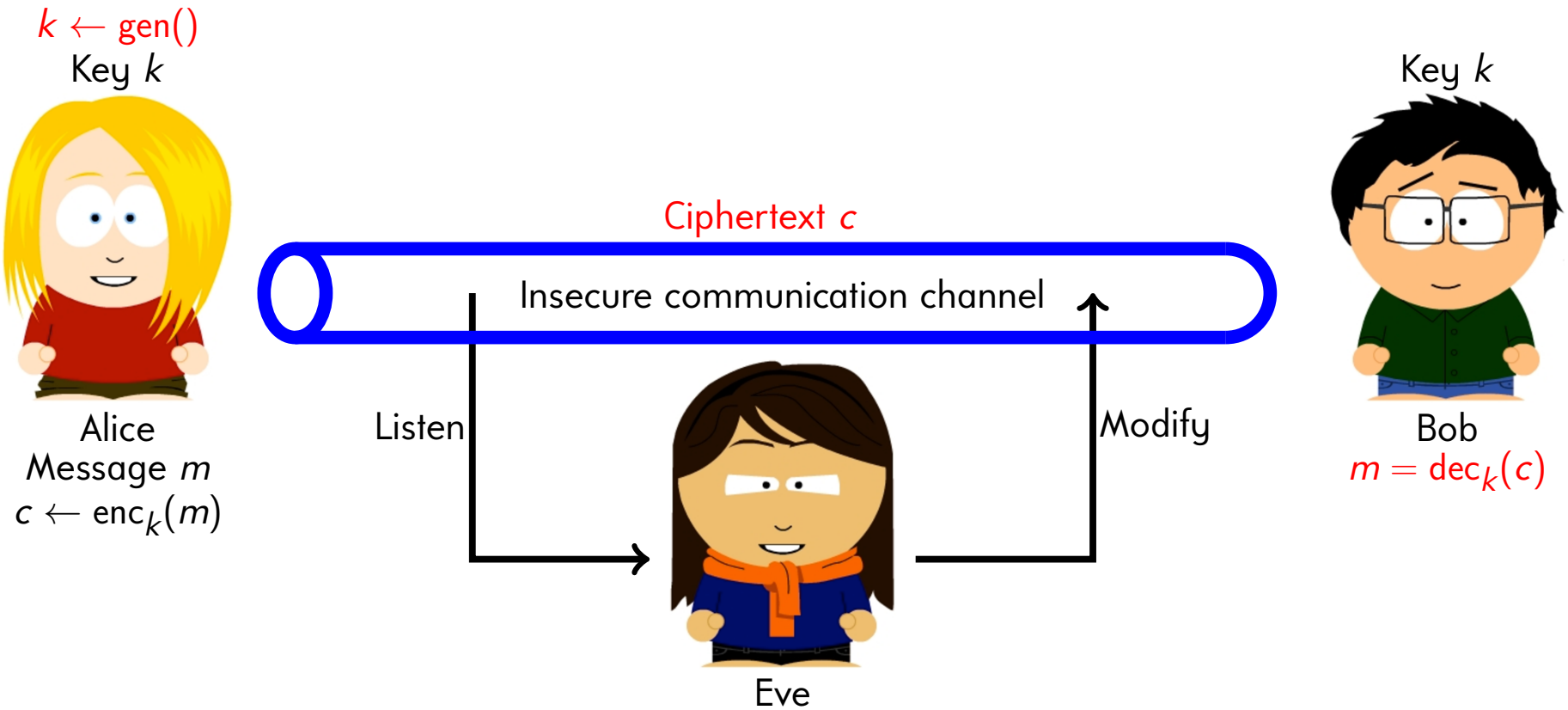
Perfectly Secret Encryption



Perfectly Secret Encryption



Perfectly Secret Encryption



Perfectly Secret Encryption

§2.5 Definition (Perfectly secret)

Encryption scheme $\mathcal{E} = (\mathsf{gen}, \mathsf{enc}, \mathsf{dec})$ is perfectly secret
if for all messages $m, m' \in \mathcal{M}$ and ciphertexts $c \in \mathcal{C}$

$$\sum_{k \in \mathcal{K}} \mathsf{P}_{\mathcal{K}}(k) \cdot \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m)\right] = \sum_{k \in \mathcal{K}} \mathsf{P}_{\mathcal{K}}(k) \cdot \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m')\right]$$

Perfectly Secret Encryption

§2.5 Definition (Perfectly secret)

Encryption scheme $\mathcal{E} = (\mathsf{gen}, \mathsf{enc}, \mathsf{dec})$ is perfectly secret
if for all messages $m, m' \in \mathcal{M}$ and ciphertexts $c \in \mathcal{C}$

$$\sum_{k \in \mathcal{K}} \mathsf{P}_{\mathcal{K}}(k) \cdot \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m)\right] = \sum_{k \in \mathcal{K}} \mathsf{P}_{\mathcal{K}}(k) \cdot \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m')\right]$$

Notes

- Probability of ciphertext c is invariant under given message m

Perfectly Secret Encryption

§2.5 Definition (Perfectly secret)

Encryption scheme $\mathcal{E} = (\mathsf{gen}, \mathsf{enc}, \mathsf{dec})$ is perfectly secret if for all messages $m, m' \in \mathcal{M}$ and ciphertexts $c \in \mathcal{C}$

$$\sum_{k \in \mathcal{K}} \mathsf{P}_{\mathcal{K}}(k) \cdot \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m)\right] = \sum_{k \in \mathcal{K}} \mathsf{P}_{\mathcal{K}}(k) \cdot \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m')\right]$$

Notes

- Probability of ciphertext c is invariant under given message m
- We let $O_{\mathcal{E}}(c, m) = \sum_{k \in \mathcal{K}} \mathsf{P}_{\mathcal{K}}(k) \cdot \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m)\right]$
- Simplifies to $\sum_{k \in \mathcal{K}} \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m)\right] = \sum_{k \in \mathcal{K}} \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m')\right]$ for uniform key distribution $\mathsf{P}_{\mathcal{K}}$

Perfectly Secret Encryption

Vigenère cipher with uniformly distributed keys of length 2

- Let $\mathsf{P}_K(b_1 b_2) = \frac{1}{4}$ (uniform key distribution)
- Consider ciphertext $c = 11$ and messages $m = 00$ and $m' = 01$

Perfectly Secret Encryption

Vigenère cipher with uniformly distributed keys of length 2

- Let $\mathsf{P}_K(b_1 b_2) = \frac{1}{4}$ (uniform key distribution)
- Consider ciphertext $c = 11$ and messages $m = 00$ and $m' = 01$

$$\sum_{k \in K} \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m)\right] = 1$$

Perfectly Secret Encryption

Vigenère cipher with uniformly distributed keys of length 2

- Let $\mathsf{P}_K(b_1 b_2) = \frac{1}{4}$ (uniform key distribution)
- Consider ciphertext $c = 11$ and messages $m = 00$ and $m' = 01$

$$\sum_{k \in K} \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m)\right] = 1 = \sum_{k \in K} \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m')\right]$$

Perfectly Secret Encryption

Vigenère cipher with uniformly distributed keys of length 2

- Let $\mathsf{P}_K(b_1 b_2) = \frac{1}{4}$ (uniform key distribution)
- Consider ciphertext $c = 11$ and messages $m = 00$ and $m' = 01$

$$\sum_{k \in K} \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m)\right] = 1 = \sum_{k \in K} \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m')\right]$$

- Consider ciphertext $c = 000$ and messages $m = 000$ and $m' = 001$

Perfectly Secret Encryption

Vigenère cipher with uniformly distributed keys of length 2

- Let $\mathsf{P}_K(b_1 b_2) = \frac{1}{4}$ (uniform key distribution)
- Consider ciphertext $c = 11$ and messages $m = 00$ and $m' = 01$

$$\sum_{k \in K} \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m)\right] = 1 = \sum_{k \in K} \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m')\right]$$

- Consider ciphertext $c = 000$ and messages $m = 000$ and $m' = 001$

$$\sum_{k \in K} \mathsf{P}\left[c \leftarrow \mathsf{enc}_k(m)\right] = 1$$

Perfectly Secret Encryption

Vigenère cipher with uniformly distributed keys of length 2

- Let $\mathsf{P}_K(b_1 b_2) = \frac{1}{4}$ (uniform key distribution)
- Consider ciphertext $c = 11$ and messages $m = 00$ and $m' = 01$

$$\sum_{k \in K} \mathsf{P}\left[c \leftarrow \mathrm{enc}_k(m)\right] = 1 = \sum_{k \in K} \mathsf{P}\left[c \leftarrow \mathrm{enc}_k(m')\right]$$

- Consider ciphertext $c = 000$ and messages $m = 000$ and $m' = 001$

$$\sum_{k \in K} \mathsf{P}\left[c \leftarrow \mathrm{enc}_k(m)\right] = 1 \neq 0 = \sum_{k \in K} \mathsf{P}\left[c \leftarrow \mathrm{enc}_k(m')\right]$$

- Encryption scheme not perfectly secret

Perfectly Secret Encryption

§2.6 Definition (Scenario)

Scenario is pair $(\mathcal{E}, \mathsf{P}_{\mathcal{M}})$ of private-key encryption scheme $\mathcal{E}$ and probability distribution $\mathsf{P}_{\mathcal{M}} \colon \mathcal{M} \to [0,1]$.

Perfectly Secret Encryption

§2.6 Definition (Scenario)

Scenario is pair $(\mathcal{E}, \mathsf{P}_{\mathcal{M}})$ of private-key encryption scheme $\mathcal{E}$ and probability distribution $\mathsf{P}_{\mathcal{M}} \colon \mathcal{M} \to [0,1]$. Define $\mathsf{P}_C \colon C \to [0,1]$ for all $c \in C$ by

$$\mathsf{P}_C(c) = \sum_{k \in K, m \in \mathcal{M}} \mathsf{P}_K(k) \cdot \mathsf{P}_{\mathcal{M}}(m) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big]$$

Perfectly Secret Encryption

§2.6 Definition (Scenario)

Scenario is pair $(\mathcal{E}, \mathsf{P}_M)$ of private-key encryption scheme $\mathcal{E}$ and probability distribution $\mathsf{P}_M \colon M \to [0,1]$. Define $\mathsf{P}_C \colon C \to [0,1]$ for all $c \in C$ by

$$\mathsf{P}_C(c) = \sum_{k \in K, m \in M} \mathsf{P}_K(k) \cdot \mathsf{P}_M(m) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big]$$

Note for perfectly secret encryption scheme and some $m' \in M$

$$\begin{aligned} \mathsf{P}_C(c) &= \sum_{k \in K, m \in M} \mathsf{P}_K(k) \cdot \mathsf{P}_M(m) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] \\ &= \sum_{m \in M} \mathsf{P}_M(m) \cdot \Big(\sum_{k \in K} \mathsf{P}_K(k) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] \Big) \end{aligned}$$

Perfectly Secret Encryption

§2.6 Definition (Scenario)

Scenario is pair $(\mathcal{E}, \mathsf{P}_M)$ of private-key encryption scheme $\mathcal{E}$ and probability distribution $\mathsf{P}_M \colon M \to [0,1]$. Define $\mathsf{P}_C \colon C \to [0,1]$ for all $c \in C$ by

$$\mathsf{P}_C(c) = \sum_{k \in K, m \in M} \mathsf{P}_K(k) \cdot \mathsf{P}_M(m) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big]$$

Note for perfectly secret encryption scheme and some $m' \in M$

$$\begin{aligned}
\mathsf{P}_C(c) &= \sum_{k \in K, m \in M} \mathsf{P}_K(k) \cdot \mathsf{P}_M(m) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] \\
&= \sum_{m \in M} \mathsf{P}_M(m) \cdot \Big(\sum_{k \in K} \mathsf{P}_K(k) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] \Big) \\
&= \sum_{m \in M} \mathsf{P}_M(m) \cdot O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m') \cdot \sum_{m \in M} \mathsf{P}_M(m) = O_{\mathcal{E}}(c, m')
\end{aligned}$$

Perfectly Secret Encryption

§2.6 Definition (Scenario)

Scenario is pair $(\mathcal{E}, \mathsf{P}_M)$ of private-key encryption scheme $\mathcal{E}$ and probability distribution $\mathsf{P}_M \colon M \to [0,1]$. Define $\mathsf{P}_C \colon C \to [0,1]$ for all $c \in C$ by

$$\mathsf{P}_C(c) = \sum_{k \in K, m \in M} \mathsf{P}_K(k) \cdot \mathsf{P}_M(m) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big]$$

Note for perfectly secret encryption scheme and some $m' \in M$

$$\begin{aligned}
\mathsf{P}_C(c) &= \sum_{k \in K, m \in M} \mathsf{P}_K(k) \cdot \mathsf{P}_M(m) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] \\
&= \sum_{m \in M} \mathsf{P}_M(m) \cdot \Big(\sum_{k \in K} \mathsf{P}_K(k) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] \Big) \\
&= \sum_{m \in M} \mathsf{P}_M(m) \cdot O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m') \cdot \sum_{m \in M} \mathsf{P}_M(m) = O_{\mathcal{E}}(c, m')
\end{aligned}$$

Perfectly Secret Encryption

§2.6 Definition (Scenario)

Scenario is pair $(\mathcal{E}, \mathsf{P}_M)$ of private-key encryption scheme $\mathcal{E}$ and probability distribution $\mathsf{P}_M \colon M \to [0,1]$. Define $\mathsf{P}_C \colon C \to [0,1]$ for all $c \in C$ by

$$\mathsf{P}_C(c) = \sum_{k \in K, m \in M} \mathsf{P}_K(k) \cdot \mathsf{P}_M(m) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big]$$

Note for perfectly secret encryption scheme and some $m' \in M$

$$\begin{aligned}
\mathsf{P}_C(c) &= \sum_{k \in K, m \in M} \mathsf{P}_K(k) \cdot \mathsf{P}_M(m) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] \\
&= \sum_{m \in M} \mathsf{P}_M(m) \cdot \Big(\sum_{k \in K} \mathsf{P}_K(k) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] \Big) \\
&= \sum_{m \in M} \mathsf{P}_M(m) \cdot O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m') \cdot \sum_{m \in M} \mathsf{P}_M(m) = O_{\mathcal{E}}(c, m')
\end{aligned}$$

Perfectly Secret Encryption

§2.6 Definition (Scenario)

Scenario is pair $(\mathcal{E}, \mathsf{P}_M)$ of private-key encryption scheme $\mathcal{E}$ and probability distribution $\mathsf{P}_M \colon M \to [0,1]$. Define $\mathsf{P}_C \colon C \to [0,1]$ for all $c \in C$ by

$$\mathsf{P}_C(c) = \sum_{k \in K, m \in M} \mathsf{P}_K(k) \cdot \mathsf{P}_M(m) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big]$$

Note for perfectly secret encryption scheme and some $m' \in M$

$$\begin{aligned}
\mathsf{P}_C(c) &= \sum_{k \in K, m \in M} \mathsf{P}_K(k) \cdot \mathsf{P}_M(m) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] \\
&= \sum_{m \in M} \mathsf{P}_M(m) \cdot \Big(\sum_{k \in K} \mathsf{P}_K(k) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] \Big) \\
&= \sum_{m \in M} \mathsf{P}_M(m) \cdot O_{\mathcal{E}}(c, m) = O_{\mathcal{E}}(c, m') \cdot \sum_{m \in M} \mathsf{P}_M(m) = O_{\mathcal{E}}(c, m')
\end{aligned}$$

Perfectly Secret Encryption

Vigenère cipher with uniformly distributed keys of length 2

- Let $\mathsf{P}_{\mathcal{M}}(m_1 \cdots m_n) = \prod_{i=1}^{n} p(m_i)$ with $p(0) = \frac{2}{5}$ and $p(1) = \frac{3}{5}$
- Let $\mathsf{P}_{K}(b_1 b_2) = \frac{1}{4}$

Perfectly Secret Encryption

Vigenère cipher with uniformly distributed keys of length 2

- Let $\mathrm{P}_{\mathcal{M}}(m_1 \cdots m_n) = \prod_{i=1}^{n} p(m_i)$ with $p(0) = \frac{2}{5}$ and $p(1) = \frac{3}{5}$
- Let $\mathrm{P}_K(b_1 b_2) = \frac{1}{4}$
- 4 ways to obtain ciphertext $c = 000$

$$\begin{aligned}\mathrm{P}_C(c) &= \sum_{k \in K, m \in \mathcal{M}} \mathrm{P}_K(k) \cdot \mathrm{P}_{\mathcal{M}}(m) \cdot \mathrm{P}\left[c \leftarrow \mathrm{enc}_k(m)\right] \\ &= \mathrm{P}_K(00) \cdot \mathrm{P}_{\mathcal{M}}(000) + \mathrm{P}_K(01) \cdot \mathrm{P}_{\mathcal{M}}(010) + \\ &\quad \mathrm{P}_K(10) \cdot \mathrm{P}_{\mathcal{M}}(101) + \mathrm{P}_K(11) \cdot \mathrm{P}_{\mathcal{M}}(111)\end{aligned}$$

Perfectly Secret Encryption

Vigenère cipher with uniformly distributed keys of length 2

- Let $\mathrm{P}_{\mathcal{M}}(m_1 \cdots m_n) = \prod_{i=1}^{n} p(m_i)$ with $p(0) = \frac{2}{5}$ and $p(1) = \frac{3}{5}$
- Let $\mathrm{P}_K(b_1 b_2) = \frac{1}{4}$
- 4 ways to obtain ciphertext $c = 000$

$$
\begin{aligned}
\mathrm{P}_C(c) &= \sum_{k \in K, m \in \mathcal{M}} \mathrm{P}_K(k) \cdot \mathrm{P}_{\mathcal{M}}(m) \cdot \mathrm{P}\left[c \leftarrow \mathrm{enc}_k(m)\right] \\
&= \mathrm{P}_K(00) \cdot \mathrm{P}_{\mathcal{M}}(000) + \mathrm{P}_K(01) \cdot \mathrm{P}_{\mathcal{M}}(010) + \\
&\quad \mathrm{P}_K(10) \cdot \mathrm{P}_{\mathcal{M}}(101) + \mathrm{P}_K(11) \cdot \mathrm{P}_{\mathcal{M}}(111) \\
&= \frac{1}{4} \cdot \left(\frac{2^3 + 2^2 \cdot 3 + 2 \cdot 3^2 + 3^3}{5^3} \right) = \frac{1}{4} \cdot \frac{8 + 12 + 18 + 27}{125} \\
&= \frac{1}{4} \cdot \frac{65}{125} = \frac{13}{100}
\end{aligned}
$$

Summary

- Monoalphabetic ciphers
- Vigenère cipher & its cryptanalysis
- Perfect secrecy