*Handouts*

Assignment 9


Exam 1
Monday, October 13
7 PM - ?


## 1:15pm, Axinn 229: *Oops! All Stats*
## *Chair: Christian Stratton, Assistant Professor of Statistics*

**Meaghan Winder**, Visiting Assistant Professor of Statistics
*Finding a mussel in a lake-stack: using statistics to inform early detection monitoring efforts for aquatic invasive species*

**Christian Stratton**, Assistant Professor of Statistics
*A statistical assessment of the impact of White-nose syndrome on bats in Montana*

**Alex Lyford**, Associate Professor of Statistics
*Using statistics to improve infant health outcomes*

## 2:30pm, Axinn 221: *Who's Thinking What?*
## *Chair: Michael Olinick, John C. Baldwin Professor of Mathematics and Natural Philosophy*

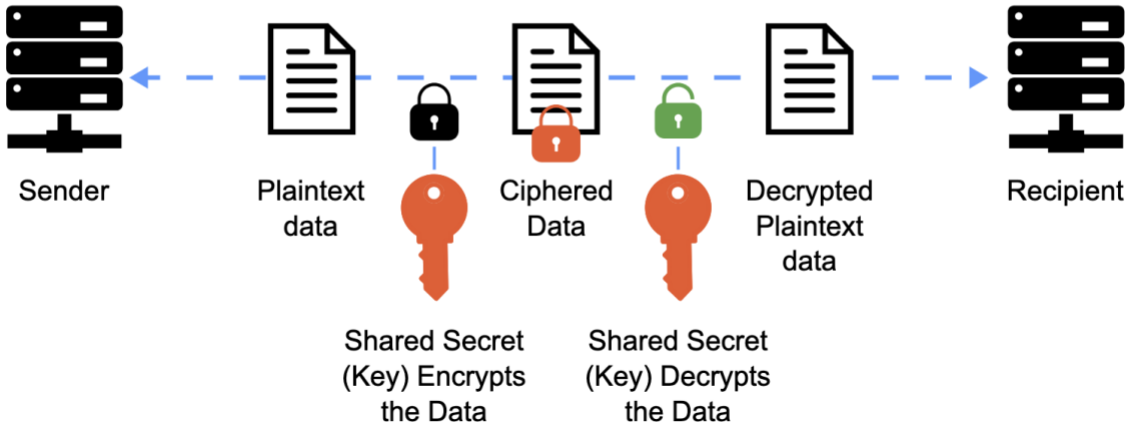
**Michael Olinick**, John C. Baldwin Professor of Mathematics and Natural Philosophy
*Can Machines Think? 75 Years of the Turing Test*

**Will Pyle**, Frederick C. Dirks Professor of International Economics
*Russian Public Opinion, the War in Ukraine, and the Lingering Effects of the Soviet Collapse*

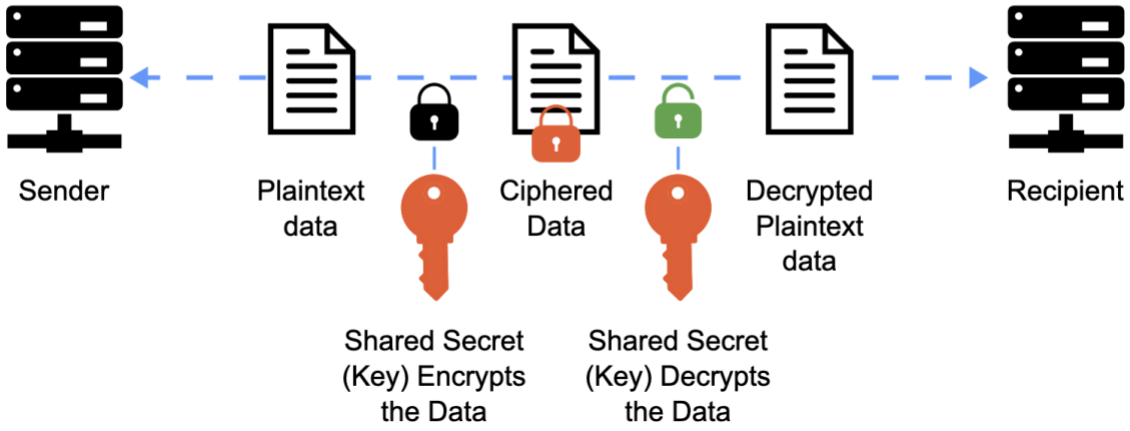
**Rose Morris-Wright**, Assistant Professor of Mathematics
*Reflections in Geometry and Algebra*

# Public Key Cryptology

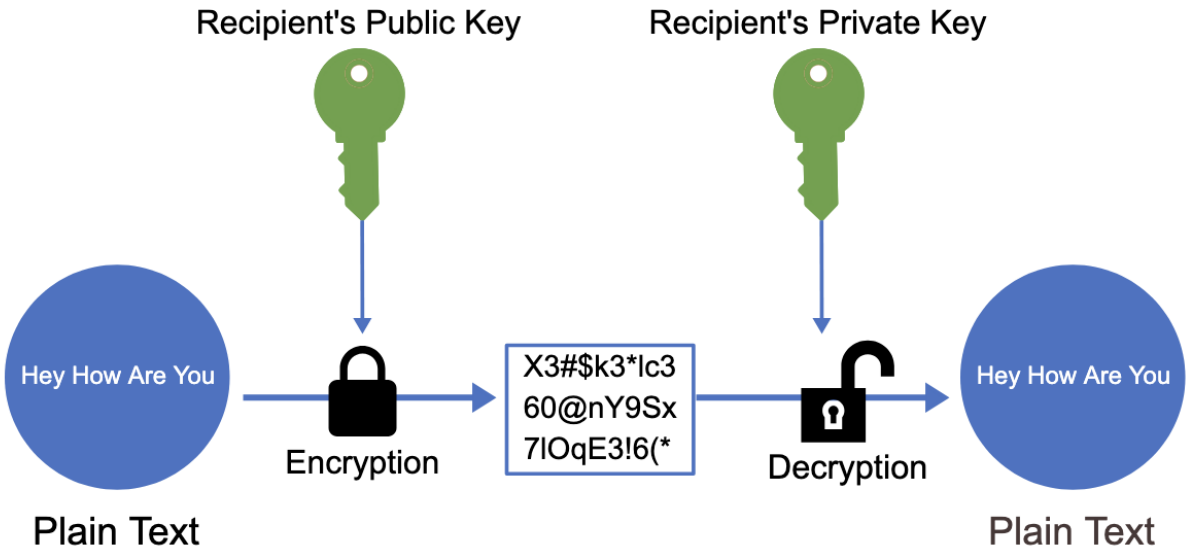
# Private Key Encryption (Symmetric)



# Private Key Encryption (Symmetric)




# Public Key Encryption



# How Close Was Turing to Public-Key Cryptology?

DIED JUNE 8,1954

PRINCETON UNIVERSITY — THE GRADUATE SCHOOL

TURING, ALAN MATHISON — Enrolled 9/29/36 — Department MATHEMATICS

Date and place of birth June 23, 1912 (Paddington, London) — Single x — Married

Bachelor and other degrees B.A. University of Cambridge, 1934; Ph.D. Princeton University, 1938

Previous graduate study 1934 (July) to August 1936 University of Cambridge

Teaching experience Jan. 1935 to June 1936 Supervisor of Undergraduates, University of Cambridge

Address: Princeton 183 G.C.; 182 G.C.

Parent or Guardian and address Mr. J. M. Turing, 8 Ennismore Ave., Guildford, England.

1936-37 Fellow from King's College

1937-38 Jane Eliza Procter Visiting Fellow in Mathematics

1938- Fellow at King's College, Cambridge

A. M. or M. F. A. — Degree granted

[21-803]

Address

PH. D.

French Satisfactory May 20, 1937 — German satisfactory May 20, 1937

General Examination Passed May 26, 1937

Dissertation Subject "Systems of Logic Based on Ordinals".

Dissertation accepted May 18, 1938 — Published under

Published 1939. Printed by C.F.Hodgson and Son,Ltd.,2 Newton St., London,W.C.2,England. Copies sent University Library 1939.

Final Examination Passed May 27, 1938 — Degree granted June 21, 1938

Diploma address

# How Close Was Turing to Public-Key Cryptology?

Let's look back to the fall of 1937. Nazi Germany was rearming under Adolf Hitler, world–shattering war looked imminent, and Alan Turing was pondering the usefulness of number theory.

# How Close Was Turing to Public-Key Cryptology?

Let's look back to the fall of 1937. Nazi Germany was rearming under Adolf Hitler, world–shattering war looked imminent, and Alan Turing was pondering the usefulness of number theory.

He foresaw that preserving military secrets would be vital in the coming conflict and proposed a way to encrypt communications using number theory.

## TURING'S CIPHER (Version 1) (Ordinary Arithmetic)

Step 1: Sender (Alice) and receiver (Bob) agree on a secret key, a large prime number $p$.

Step 2: Sender translates the plain text message into a large prime number

**REBECCAS**

| R | E | B | E | C | C | A | A |
|---|---|---|---|---|---|---|---|
| 18 | 05 | 02 | 05 | 03 | 03 | 01 | 19 |

18050205030119

Append integers on the end so the result is a prime:

$$M = 1805020503011\mathbf{179}$$

Step 3: Sender enciphers $M$ by multiplying $M$ by $p$:

$$M^* = Mp$$

and transmits $M^*$

Step 4: Receiver deciphers message by dividing M* by p

Note that Sender and Receiver have **easy** tasks.

How about our Eavesdropper (Carol)?
Can she crack the ciphertext M*?

A direct attack based on factoring M* is a **hard** problem as far as we know.

So Turing appears to have an idea similar to RSA:
multiplying is easy, factoring is hard.

BUT..

BUT..

Suppose the Eavesdropper intercepts a second enciphered message from the Sender to the Receiver

$$N^* = Np$$

Observe:

1. The greatest common divisor of $N* = Np$ and $M* = Mp$ is easy to find. (The Euclidean Algorithm again)

2. The greatest common divisor of $Np$ and $Mp$ is $p$ since both $N$ and $M$ are prime numbers.

It's trivial to find the "secret" key $p$.

## TURING'S CIPHER (Version 2) *modular arithmetic*

Version 1 uses conventional arithmetic.
Version 2 uses modular arithmetic.

Step 1: Sender and receiver agree on a large prime $p$, which may be made public. They also agree on a secret key $k$, an integer less than $p$. Thus $k$ is one of the numbers 1, 2, 3, É,, $p-1$. It does not have to be a prime number.

Step 2: Sender translate plaintext into blocks of integers, each less than $p$. Let $M$ denote one of these blocks.

Step 3: Sender enciphers $M$ by computing $Mk$ and reducing the product modulo $p$.

$$Mk = M^* \bmod p$$

Sender transmits $M*$

Step 3: Sender enciphers $M$ by computing $Mk$ and reducing the product modulo $p$.

$$Mk = M^* \bmod p$$
$$\text{Sender transmits } M*$$

Step 4: How does Receiver decipher the message?

Since $k$ is a positive integer less than $p$, $k$ is relatively prime to $p$.

Thus $k$ has an inverse $j$ (modulo $p$):

The Receiver multiplies $M*$ by $j$

$$M * j = (Mk)j \bmod p = M(kj) \bmod p$$
$$= M \times 1 \bmod p = M \bmod p$$

$$\text{By Fermat's Theorem, } k^{p-1} = 1 \bmod p$$
$$\text{Thus } k^{p-2}k = 1 \bmod p \text{ so } k^{p-2} \text{ is the inverse of } k \bmod p.$$
$$\text{The receiver knows } j.$$

## Fermat's Little Theorem

Pierre de Fermat first stated the theorem in a letter dated October 18, 1640, to his friend and confidant Frénicle de Bessy as the following:

> If $p$ is a prime and $a$ is any integer not divisible by $p$, then $a^{p-1} - 1$ is divisible by $p$.

Fermat did not prove his assertion, only stating:

> Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers; de quoi je vous envoierois la démonstration, si je n'apprhendois d'étre trop long.

(And this proposition is generally true for all series and for all prime numbers; the proof of which I would send to you, if I did not fear it being too long.)

## Weakness of Turing's 2nd Cipher

## Subject to known-plaintext attack

## Weakness of Turing's 2nd Cipher
## Subject to known-plaintext attack

During World War II German weather reports were not encrypted with the supposedly highly secure Enigma system. After all, so what if the Allies learned that there was rain off the south coast of Iceland?

## Weakness of Turing's 2nd Cipher
## Subject to known-plaintext attack

During World War II German weather reports were not encrypted with the supposedly highly secure Enigma system. After all, so what if the Allies learned that there was rain off the south coast of Iceland?

This practice provided the British with a critical edge in the Atlantic naval battle during 1941.

## Weakness of Turing's 2nd Cipher
## Subject to known-plaintext attack

During World War II German weather reports were not encrypted with the supposedly highly secure Enigma system. After all, so what if the Allies learned that there was rain off the south coast of Iceland?

This practice provided the British with a critical edge in the Atlantic naval battle during 1941.

The problem was that some of those weather reports had originally been transmitted from U–boats out in the Atlantic. Thus, the British obtained both unencrypted reports and the same reports encrypted with Enigma. By comparing the two, the British were able to determine which key the Germans were using that day and could read all other Enigma encoded traffic.

Suppose our eavesdropper knows both $M$ and $M^*$ where

$$M^* = Mk \bmod p$$

$$\begin{aligned} \text{Then } M^{p-2}M^* &= M^{p-2}Mk \bmod p \\ &= M^{p-1}k \bmod p \\ &= k \bmod p \text{ by Fermat's Theorem.} \end{aligned}$$

So Carol can discover the secret key $k$ and can decrypt any message.

"Thus Turing's cipher has no practical value. Fortunately, Turing got better at cryptography after devising this code; his subsequent cracking of Enigma surely saved thousands of lives, if not the whole of Britain."

Tom Leighton and Romitt Rubinfeld