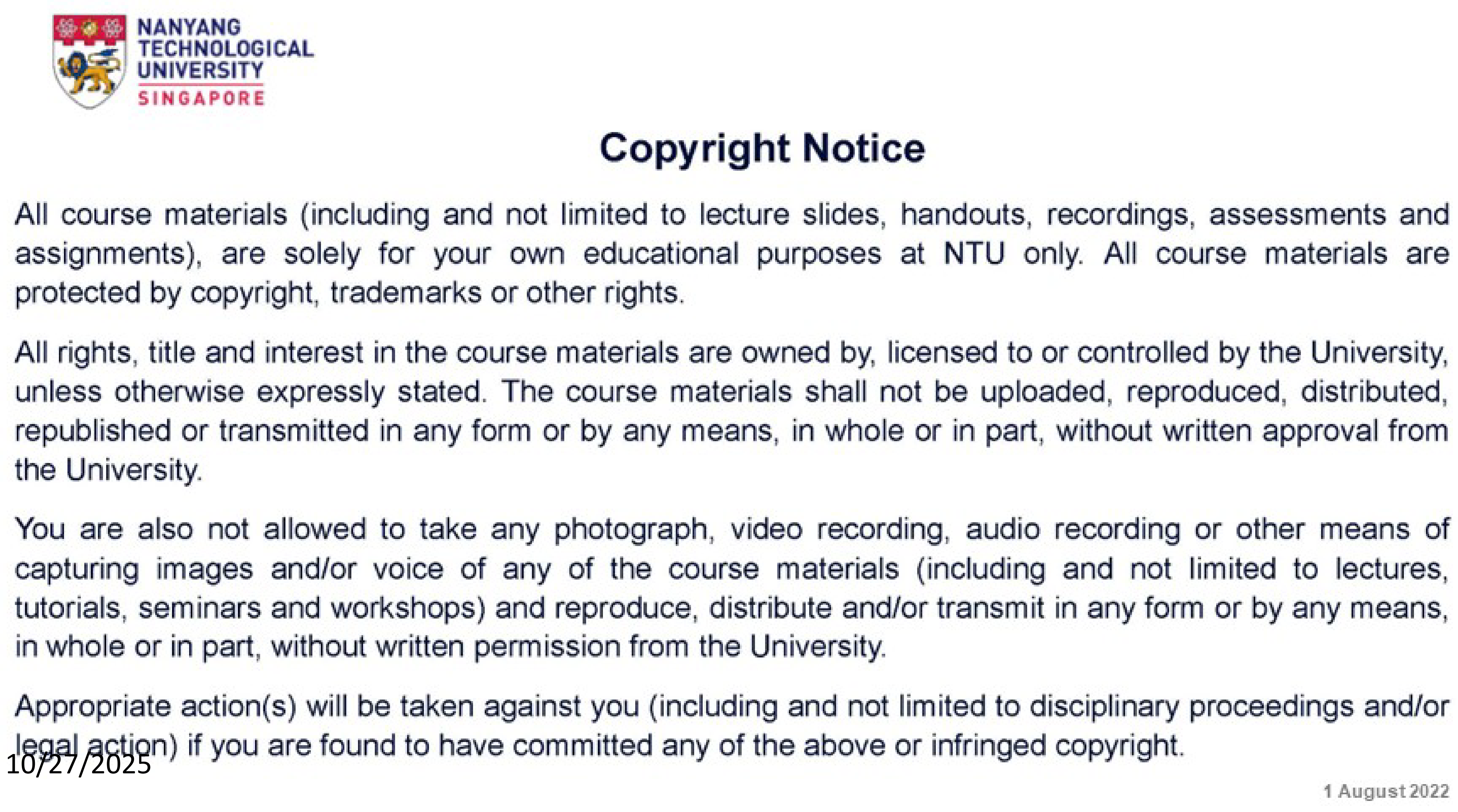
3010 Applied Crypto 2
Stream Ciphers

Dr Tay Kian Boon

NTU, CCDS

2025 Semester 1



Overview Week 2 Lectures

- Randomness
- WW2 machine ciphers
  - **PURPLE** (Japan) (wont cover)
  - **ENIGMA** (Germany)
- Stream ciphers

Randomness –Birthday Paradox

- Assuming birthdays independent. How many people is needed in a room where you can find a chance of >50% of same birthday
- Ans: only 23 (tutorial)

Randomness –Birthday Paradox

- 23 seems to be a paradoxically small number since we have 365 possible dates for birthdays
- Note 23 approx 1.2*sqrt365

Randomness –Birthday Paradox

- In early IPOD days, some listeners complained hearing same song within 2 hours although they have 400 songs on their ipod. Assuming 4 min songs on average.
- Question: Is IPOD shuffling random? (tutorial)

Historical WW2 Ciphers

- After one-time pad (which is difficult to produce), during WW1 & WW2 period, military from many big countries begin to conceive of making machine encryptors for their use

- 2 most famous ones:
  - **PURPLE ciphers (Japan)** –wont cover
  - **ENIGMA ciphers (Germany)**

What is Cryptography - Informal

- As the German military grew in the late 1920s, it began looking for a better way to secure its communications.
- They built new cryptographic machine called **'ENIGMA.'**
- **It is polyalphabetic.**
- They believed the encryption generated by the machine to be unbreakable. With a theoretical number of ciphering possibilities of 2 × 10^23 = 2^77, their belief was not unjustified.
- Broken eventually by Rejewski (Polish mathematician) & The Brits led by Alan Turing (CS father) with the help of german traitor)

The Enigma Machine: Overview

Attributed to German military during World War II

Invented by Arthur Scherbius at the end of WW-I

Key : Settings for the machine components

Wheel order, Ring settings, Plug connections, etc.

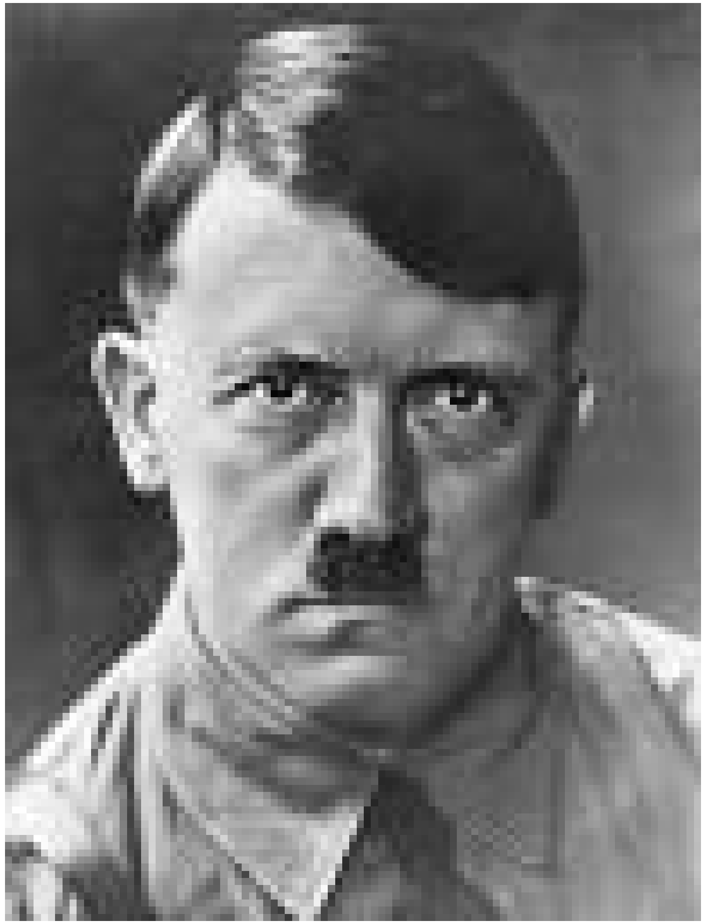
Initialization : Rotor positions chosen by operator.

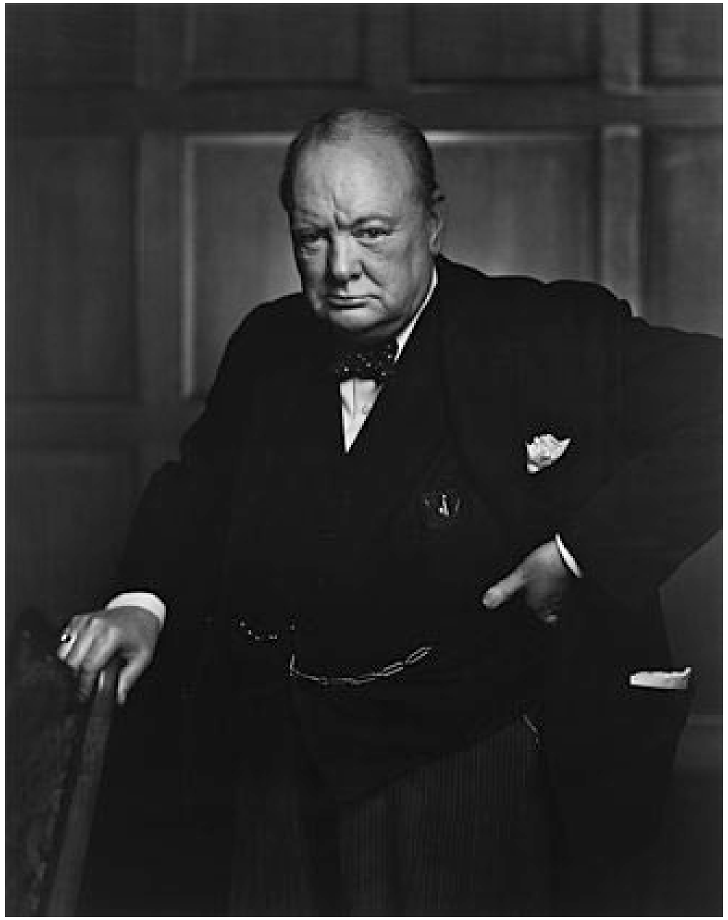
Cracking Enigma

- Cannot just be brute-forced (huge key-space)
- Extremely complicated mathematical analysis
- Needs a huge amount of computing capability
- Almost impossible without “known plaintexts”
- Kudos to Marian Rejewski et al. (1932-1939)
- And of course, Alan Turing et al. (1939-1945)

Reading : Cracking Enigma in 2021 : https://youtu.be/RzWB5jL5RX0

WW2 Fought Between them?



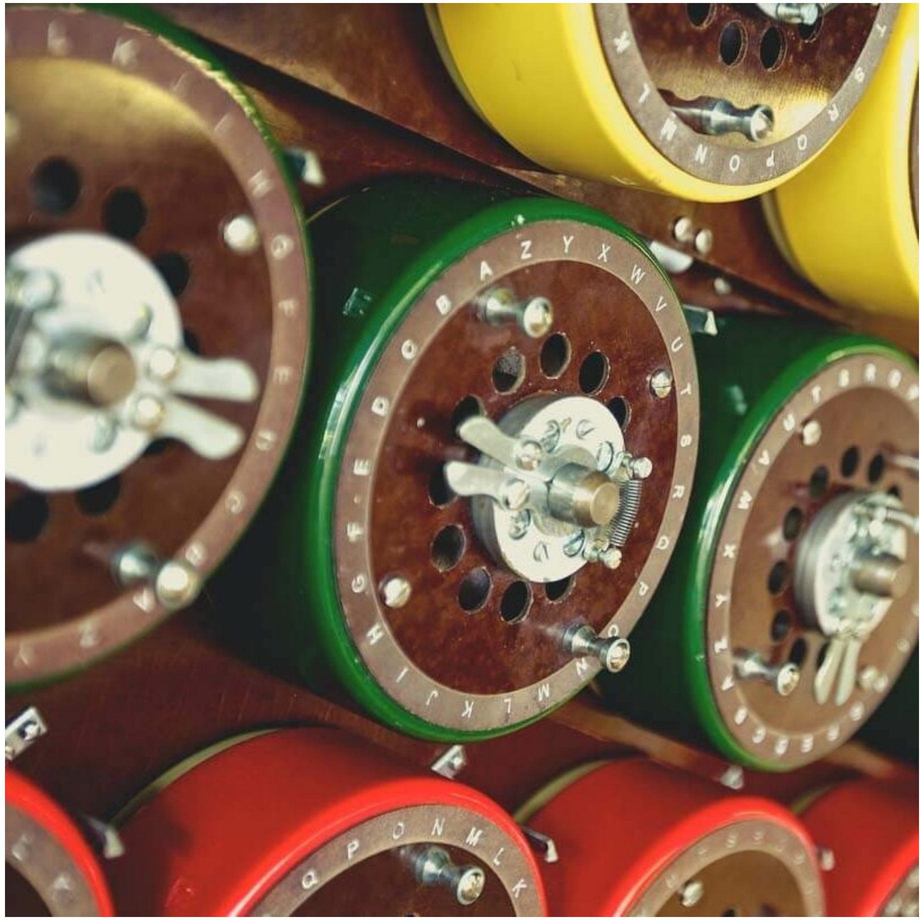


WW2 Fought Between them & Hitler!

Rejewski (1905-1980)

Turing (1912-1954)

Bletchley Park: Bombes Assembly



Facts abt Bombes

Why were the Bombes needed?

- Bletchley Park was set up to decode intercepted Nazi Engima messages. These devices typically changed settings every 24 hours and with 159 quintillion possible combinations every day, the staff at Bletchley Park worked around the clock to break the settings by hand.

- A mechanical method for identifying the keys was needed and Alan Turing designed the Bombe to speed up the process.

Factors Leading to Break of ENIGMA

- Complacency
- Careless implementation by Germans
  - Reduced settings
- Espionage
- First rate mathematicians & computer scientists
- Rich Budget

Post-WWII History

- Claude Shannon — father of the science of information theory
- Computer revolution — lots of data to protect
- Data Encryption Standard (DES), 70’s
- Public Key cryptography, 70’s
- CRYPTO conferences, 80’s
- Advanced Encryption Standard (AES), 90’s
- The crypto genie is out of the bottle…

Claude Shannon

- The founder of Information Theory
- 1949 paper: *Comm. Thy. of Secrecy Systems*
- Fundamental concepts
  - **Confusion** — obscure relationship between plaintext and ciphertext
  - **Diffusion** — spread plaintext statistics through the ciphertext
- Proved one-time pad is secure

Real-World One-Time Pad-Vernam

- Project VENONA
  - Soviet spies encrypted messages from U.S. to Moscow in 30’s, 40’s, and 50’s
  - Nuclear espionage, etc.
  - Thousands of messages
- Spy carried one-time pad into U.S.
- Spy used pad to encrypt secret messages
- Repeats within the “one-time” pads made cryptanalysis possible

SYMMETRIC CRYPTOGRAPHY

- **Symmetric Key**
  - Same key for encryption and decryption
  - 2 Modern types: **Stream ciphers, Block ciphers**
- **Stream ciphers** –– 'generalize' one-time pad
  - Except that key is relatively short
  - Key is stretched into a INFINITE (periodic) **keystream**
  - Keystream is used just like a one-time pad, **XOR the keystream with plaintext bit by bit!**
- **Block Ciphers** – later

Stream Ciphers

Stream Ciphers

- Once upon a time, not so very long ago… stream ciphers were the king of crypto
- Today, not as popular as block ciphers
- We’ll discuss some main examples stream ciphers:
- LFSRs - A5/1
  - Based on shift registers
  - Used in GSM mobile phone system (2G)
- RC4
  - Based on a changing lookup table
  - Used in many places (in the past, now downgraded)
- GRAIN – NFSR (secure non-linear feedback registers)

Stream Ciphers

- From Key K

1. Generate pseudorandom bits (by specific algorithm) –therefore deterministic, therefore not truly random

2. Then encrypt the plaintext by XORing it with the generated pseudorandom bits…

Stream Ciphers

- Stream ciphers are deterministic: Same initial seed with lead to same keystream to XOR with plaintext
  - This is a weakness
- Stream ciphers' determinism allows you to decrypt by regenerating the same pseudorandom bits used to encrypt.

Stream Cipher Operations

- A stream cipher computes KS = **SC**(K, N), encrypts as $C = P \oplus KS$, and decrypts as $P = C \oplus KS$.

- The encryption and decryption functions are the same because both do the same thing—namely, XOR bits with the keystream.

Stream Ciphers –Most common class

- Feedback Shift Registers (FSR)
- Will now explain the basic mechanism behind hardware stream ciphers, called ***feedback shift registers (FSRs).***
- Almost all hardware stream ciphers rely on FSRs in some way, whether that’s
  - the A5/1 cipher (encryption algo in 2G mobile phones) or
  - the more recent cipher Grain-128a.
- LFSR based: Initialised a k-bit seed, say (k=3) $s_0\ s_1\ s_2$
- Successive bits- XORing of some previous bits, say $s_{i+1} = s_{i-1} \oplus s_{i-2}$

Video Example LFSR

- See 3:22 minute onward (intro to LFSR)

https://www.youtube.com/watch?v=8fhNPXus4-s

Stream Ciphers

- Stream ciphers were popular in the past
  - Efficient in hardware
  - Speed was needed to keep up with voice, etc.
  - Today, processors are fast, so software-based crypto is usually more than fast enough
- Future of stream ciphers?
  - Expert Shamir declared “the death of stream ciphers” around 2004 (esp if its linear)

eStream Project

- The eSTREAM project was a multi-year effort, running from 2004 to 2008, to promote the design of efficient and compact stream ciphers suitable for widespread adoption.
- As a result of the project, a portfolio of new stream ciphers was announced in April 2008. The eSTREAM portfolio was revised in September 2008, and currently contains seven stream ciphers.
- This website (below) is dedicated to ciphers in this final portfolio. For information on the eSTREAM *project* and selection process, including a timetable of the project and further technical background, please visit the original eSTREAM Project website.

eStream Finalists

Profile 1 (SW)

HC-128 (Wu Hong Jun,SPMS)

Rabbit

Salsa20/12

SOSEMANUK

Profile 2 (HW)

Grain v1

MICKEY 2.0

Trivium