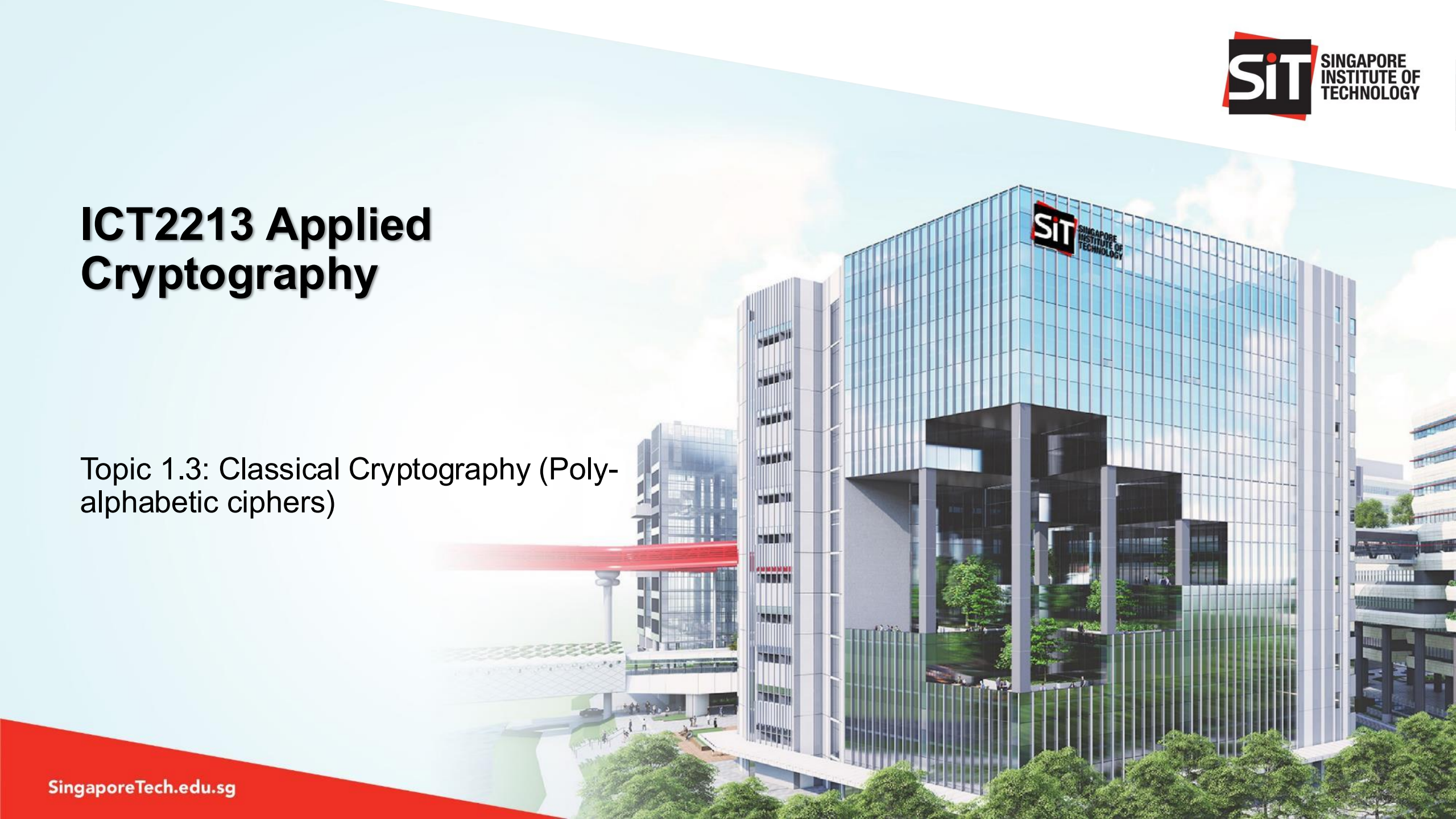
ICT2213 Applied Cryptography

Topic 1.3: Classical Cryptography (Poly-alphabetic ciphers)



Learning outcomes

- Explain how classical poly-alphabetic ciphers, such as the Vigenère and one-time pad ciphers, work
- Cryptanalyze the Vigenère cipher

The one-time pad (OTP) cipher (aka Vernam cipher)

SINGAPORE INSTITUTE OF TECHNOLOGY

Operation

- The key is a large non-repeating set of truly random letters
- The sender uses each key letter on the pad to encrypt exactly one plaintext character
- Encryption is the same as in the shift cipher
- The receiver has an identical key to decrypt the ciphertext

Example

- Assume the plaintext is **onetimepad**
- Assume the key sequence is **tbfrgfarfm**
- The resulting ciphertext is **HOJKOREGFP**
- The first key letter is t, which corresponds to number 19
- Therefore, character o is shifted 19 positions and wraps around to H

Properties of the OTP cipher

SINGAPORE INSTITUTE OF TECHNOLOGY

Poly-alphabetic cipher

- The OTP cipher is a poly-alphabetic cipher
- Each character of the plaintext can be mapped to any character of the alphabet
- This is because the shift value depends on the letter that is next on the key sequence

Unconditionally secure

- The OTP cipher is the only known provably secure cipher
- If used correctly, it cannot be broken
- The reason is that a given ciphertext is equally likely to correspond to any plaintext of equal size
- Because all keys are equally possible
- However, it is nearly impossible to use OTP correctly

The Vigenère cipher

- The Vigenère cipher is an OTP with a periodic key
- The key for Vigenère is a string of characters which is repeated until the string of copies is as long as the message
- Encryption is identical to the OTP cipher
- An example can be seen below, where the key is the word **dog**
- In this example
  - The 0th, 3rd, 6th, 9th,. . . characters are shifted by 3
  - The 1st, 4th, 7th, 10th,. . . characters are shifted by 14
  - The 2nd, 5th, 8th, 11th,. . . characters are shifted by 6

Plaintext:	helloworldoutthere
Key:	dogdogdogdogdogdog
Ciphertext:	KSROCCRFRGCAWHNHFK

Properties of the Vigenère cipher

SINGAPORE INSTITUTE OF TECHNOLOGY

Poly-alphabetic cipher

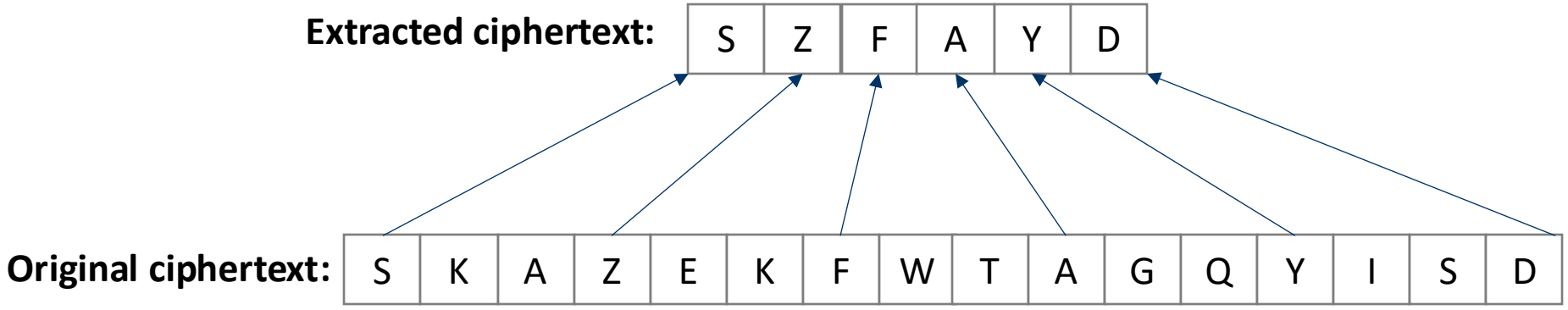
- The Vigenère cipher is a poly-alphabetic cipher
- A given letter of the plaintext can be encrypted in different ways, depending on where it falls in the message
- This messes up inter-letter statistics, and also flattens single-letter frequency statistics

Completely broken

- Despite its poly-alphabetic nature, the Vigenère cipher is very easy to break.
- The main drawback is the periodic structure of the key
- Once the length of the key is known, Vigenère is as secure as a simple shift cipher

Cryptanalysis of the Vigenère cipher

- Assume that the key length is T (sometimes called the period)
- Then, the ciphertext can be divided into T parts
- Each part can be viewed as being encrypted using a single instance of the shift cipher
- In the example below, assume that the key length is 3 (maybe an incorrect assumption)
- Then, if we extract the 0th, 3rd, 6th, 9th, 12th, and 15th characters, they are all supposed to be encrypted under the same key (shift cipher)
- In other words, the IOC for the extracted ciphertext should be ≈ 0.065



Determining the key length

- For period T = 1, 2, 3, …, up to a large enough value, extract the sequence of ciphertext characters at positions 0, T, 2T, 3T, …
- Compute the probability vector q for the individual ciphertext letters of the extracted sequence
- Compute the IOC for vector q (sum of q_i squared)
- Once you have all the IOCs for different values of period T, look for a pattern
- When T = s, 2s, 3s, .., where s is the actual key length, we expect the IOCs to be ≈0.065 (or be slightly larger than the values around them)
- Once the key length s is established, decrypt the ciphertext by using s instances of the shift cipher decryption module