



WEEK 2B

FORMAL SECURITY NOTIONS

SE 4472 - Information Security



Western
Engineering



WHISPER
LAB

LEAKING INFORMATION



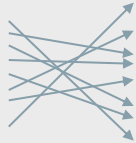
CAESAR

Reveals plaintext patterns (repeated letters) and frequency information



VIGENÈRE

Still reveals patterns and frequency information due to passphrase repetition



ENIGMA

Leaks information about what the plaintext isn't

THE PERFECT CIPHER?



CAN WE BUILD A CIPHER THAT
LEAKED NO INFORMATION?

THE ONE-TIME PAD

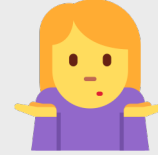
VIGENÈRE, EXCEPT...

- Key is exactly the same length as the message
- Key is uniformly random. (Every key in the keyspace is equally likely to be chosen)
- Key is never reused. EVER.

$$\begin{array}{r} \text{helloworld} \\ + \text{xwbzuojs} \\ \hline \text{eamkikxjpf} \end{array}$$

THE ONE-TIME PAD

WHICH
PLAINTEXT
WAS IT??



goodbyepal
+ ymyhhmtupu

eamkikxjpf

helloworld
+ xwbzuojssec

eamkikxjpf

noavacados
+ rmmpiixgbn

eamkikxjpf

whatsupbro
+ itmrrqqiiyr

eamkikxjpf

attacksoon
+ ehtkgafvbs

eamkikxjpf

INFORMATION-THEORETIC SECURITY

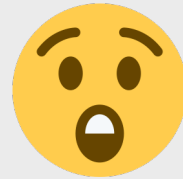
GUESSING STRATEGY

**CIPHERTEXT + KEY GUESS
= PLAINTEXT GUESS**

BUT ALL KEYS ARE EQUALLY LIKELY. SO WITHOUT ANY
OTHER INFORMATION, ALL PLAINTEXTS ARE EQUALLY
LIKELY. NO INFORMATION ABOUT PLAINTEXT IS REVEALED

INFORMATION-THEORETIC SECURITY

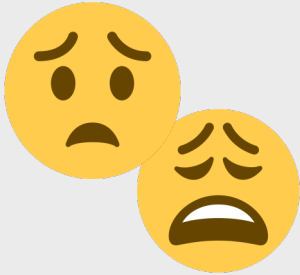
= UNBREAKABLE*



* All the computers and all the time in the universe won't help you guess the right key

INFORMATION-THEORETIC SECURITY

YOU ONLY HAVE TO...



- **SOMEHOW** securely transmit one byte of key for EVERY byte of plaintext you want to send
- **SOMEHOW** securely store one byte of key for EVERY byte of plaintext you want to receive
- **SOMEHOW** enforce you never ever reuse a single key byte EVER

COMPUTATIONAL SECURITY

**IN PRACTICE WE WANT
SHORT, FIXED-LENGTH,
REUSABLE KEYS**



FORMALIZING COMPUTATIONAL SECURITY

What should it mean for a cipher to be secure?

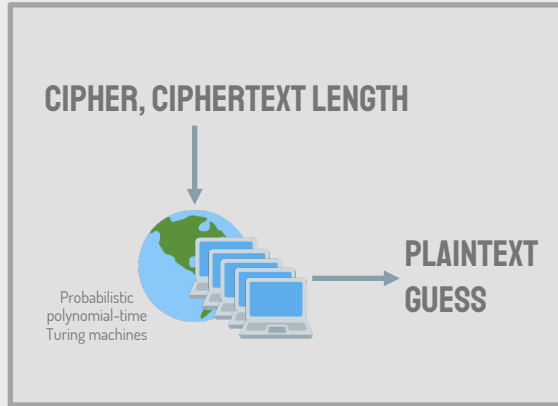
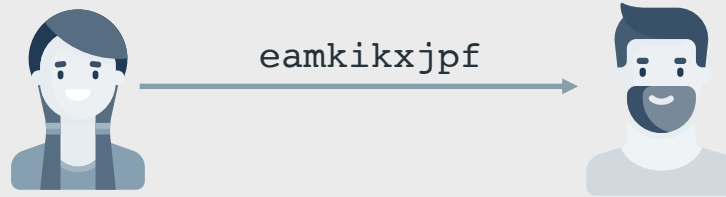
$$\pi f(x^2) \leq \{y^2\} \sum_i \left[\rho^n \times \alpha_k \neq q \right] \mu_i \dots \mu_k$$



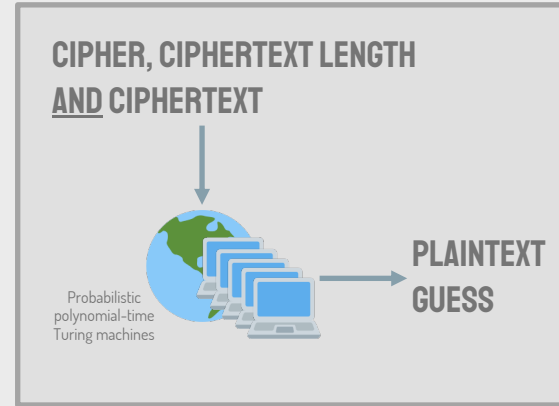
ONE-TIME PAD REVEALS NO
INFORMATION ABOUT PLAINTEXT.

CAN WE CAPTURE A SIMILAR IDEA
IN THE COMPUTATIONAL MODEL?

SEMANTIC SECURITY



UNIVERSE A

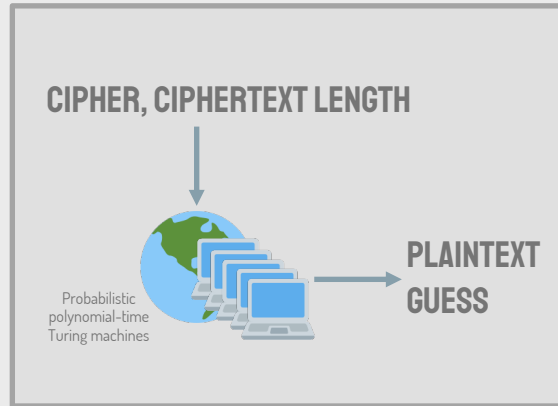


UNIVERSE B

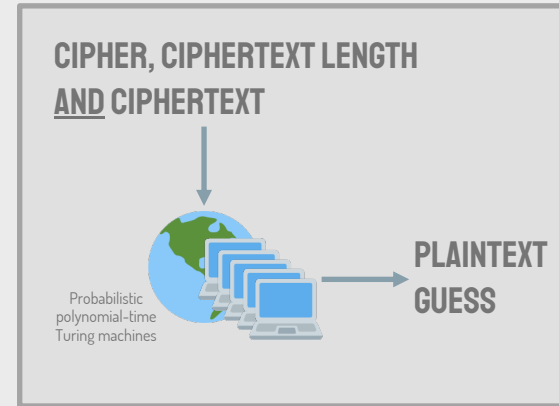
SEMANTIC SECURITY

UNIVERSE B HAS AN ADVANTAGE OVER **UNIVERSE A**

...BUT IT'S *SO SMALL*, IT'S NEGLIGIBLE



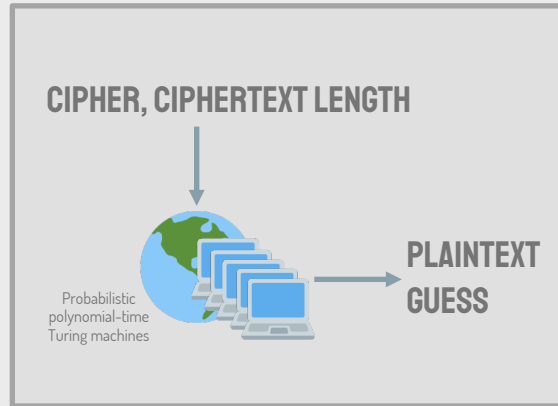
UNIVERSE A



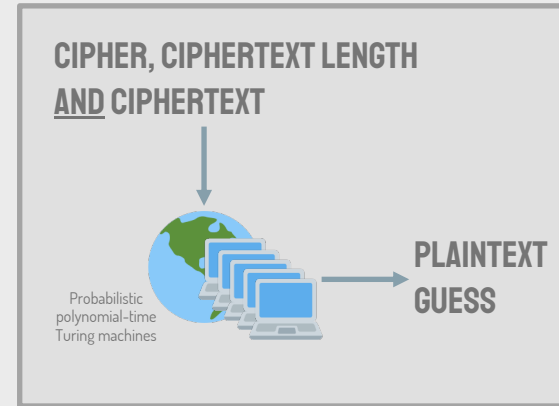
UNIVERSE B

SEMANTIC SECURITY

IN OTHER WORDS, THE KNOWING
CIPHERTEXT DOESN'T HELP THE ATTACKER



UNIVERSE A




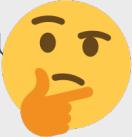


UNIVERSE B



HOW CAN WE PROVE A CIPHER IS
(OR ISN'T) SEMANTICALLY
SECURE?

LET'S PLAY A GAME

1. I pick and send you two “challenge messages”, M1, M2 
2. You flip a coin: heads you pick M1, tails you pick M2. You encrypt it and send me the “challenge ciphertext” 

3. I guess which message you picked. If I'm right, I win 

WE'LL CALL THIS THE
EVEASDROPPING (EAV) GAME



IMPLICATIONS OF THE “EAV” GAME

1. If I guess randomly, I win 50% of the time



2. If I can *distinguish* ciphertexts, I can win more than 50% of the time



3. If I can't distinguish ciphertexts, I can't do better than random guessing



IMPLICATIONS OF THE “EAV” GAME

If I win less than 50% of the time, I can always just guess the opposite, and win *more* than 50% of the time



ADVANTAGE

$$\text{Adv} = \left| \text{Pr}(\text{guessing correctly}) - \frac{1}{2} \right|$$

ADVANTAGE IS HOW FAR OFF 50% MY
SUCCESS RATE IS



IS MY ADVANTAGE EVER ZERO IN THE “EAV” GAME?

No. I get the ciphertext, so I can try to brute-force decrypt it, and will succeed with some non-zero probability

**HOW SMALL IS “SO SMALL, IT’S OF
NO PRACTICAL CONSEQUENCE?”**

NEGLIGIBLE FUNCTION

$\varepsilon(\lambda)$ is a negligible function in security parameter λ
if for every polynomial function $\text{poly}()$, there is some $\lambda' > \lambda$ such that:

$$\varepsilon(\lambda) \leq \left| \frac{1}{\text{poly}(\lambda)} \right|$$

In other words, a negligible function shrinks faster than the
inverse of any polynomial function

NEGLIGIBLE ADVANTAGE

WE HAVE A NEGLIGIBLE ADVANTAGE OF WINNING THE
“EAV” GAME IF

$$\text{Adv} \leq \varepsilon(\lambda)$$

INDISTINGUISHABILITY OF ENCRYPTION



IND-EAV SECURITY

A cipher is indistinguishable under eavesdropping (IND-EAV secure) if there exists no probabilistic polynomial-time Turing machine that can win the EAV game with a non-negligible advantage

INDISTINGUISHABILITY OF ENCRYPTION



IND-EAV EXERCISE

Prove the Caesar, Vigenère and Enigma ciphers are not IND-EAV secure

Which challenge messages would you pick? What strategy would you use to distinguish ciphertexts? What advantage would this strategy give you?

INDISTINGUISHABILITY OF ENCRYPTION

IND-EAV IS TOO STRONG

It's unrealistic in practice to assume eavesdropping is the best an attacker can do. Let's explore other attack games that grant the guesser more powers

INDISTINGUISHABILITY OF ENCRYPTION



IND-CPA SECURITY

The **chosen-plaintext attack** (CPA) game runs exactly the same as the eavesdropping game except the guesser gets an additional “power:” the ability to make encryption queries under the same key used to create the challenge ciphertext

INDISTINGUISHABILITY OF ENCRYPTION



IND-CCA1 SECURITY

The **chosen-ciphertext attack** (CCA1) game runs exactly the same as the CPA game except the guesser gets an additional “power:” the ability to make decryption queries under the same key as the challenge ciphertext, until the challenge ciphertext is received

INDISTINGUISHABILITY OF ENCRYPTION



IND-CCA2 SECURITY

The *adaptive chosen-ciphertext attack* (CCA2) game runs exactly the same as the CCA1 game except the guesser gets an additional “power:” the ability to make decryption queries after the challenge ciphertext is received*

*Decryption queries involving the challenge ciphertext, or any string outside of the ciphertext space are ignored



QUESTIONS?

Contact Prof. Essex:

aessex@uwo.ca

[@alessex](https://twitter.com/aleksessex)

See course website for slides and videos:

<https://whisperlab.org/security>

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik** and illustrations by **Stories**

Please keep this slide for attribution.