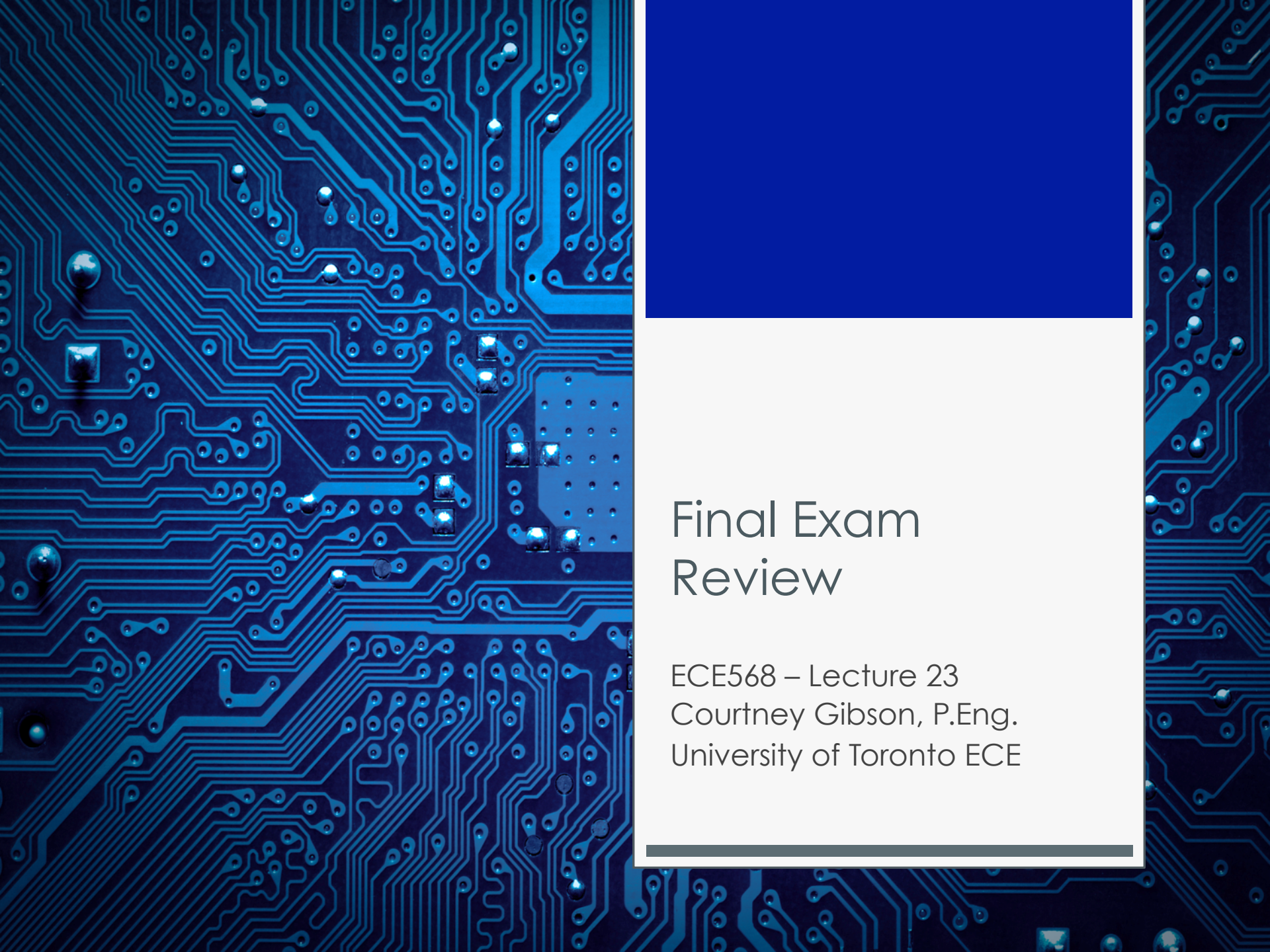


Final Exam Review

ECE568 – Lecture 23

Courtney Gibson, P.Eng.
University of Toronto ECE

Assignment #2

What is the keyspace of a polyalphabetic cipher, based on a 47-character alphabet, with a period of 3?

SYN Flooding

SYN flooding is a Denial of Service attack that exhausts what resource on the victim machine?

ARP Poisoning

For ARP poisoning to be feasible, do the attacker and victim need to be on the same subnet?

SSL Protocol

Are clients authenticated in the SSL protocol?

Covert Channels

Explain how covert channels can compromise a system's security.

Hashing

What's the difference between **pre-image resistance** and **2nd pre-image resistance**?

Format String Attacks

Which of these statements are vulnerable to a format string attack?

```
printf(buffer);
printf("%s", buffer);
```

Message Signing

In general terms, how is a signature generated in public-key cryptography?

Signatures

A new web service SignMe allows people to sign web pages. The service appends a special hidden HTML tag at the bottom of an otherwise normal web page. The tag contains the author's name, the date, and a signature (which contains the author's name and date signed by the author's RSA private key). The web page is unencrypted, but the signature can be validated by downloading http://www.signme.com/keys.html (which contains a list of all registered SignMe users and each user's public key) to retrieve the author's public key.

BGP

Describe how BGP can be exploited, and what the resulting attack would accomplish.

Spam

Describe how a spammer could utilize a botnet to avoid blacklist filters.

DNS

Describe two types of attack involving DNS cache poisoning that involve sending spoofed DNS responses.

Malware

What is a key difference between a virus and a worm?

Kerberos

Explain the roles of the authentication server and the ticket-granting server in Kerberos.

Worms

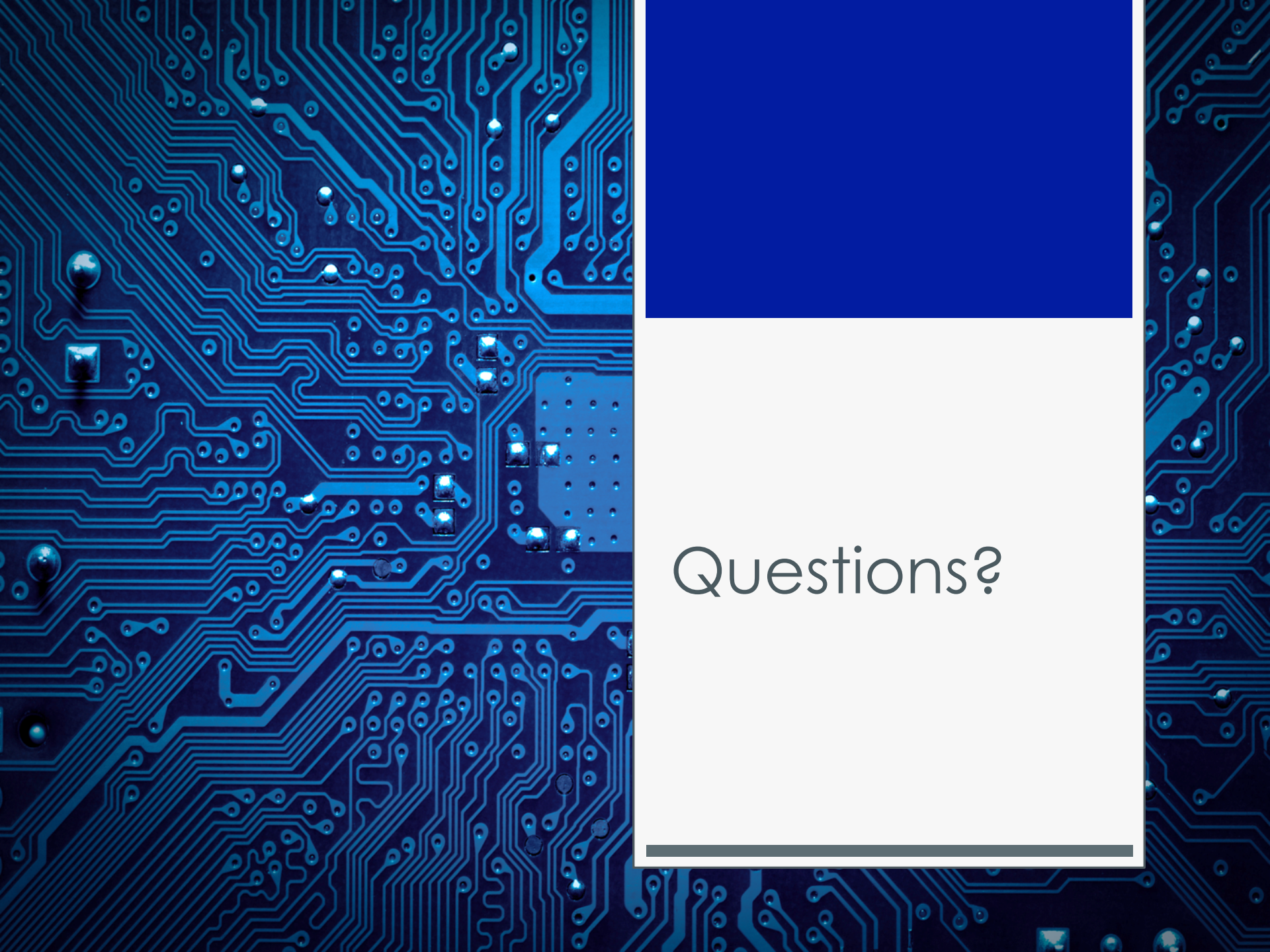
What is a “hit-list”, in the context of worms, and why are they used?

Rootkits

Explain a technique that a rootkit might use, in order to prevent its files from showing up in a directory listing.

Spam

Explain how anti-spam graylists work.


Questions?