calyptix® SECURITY

ascii the ascii group® inc. The IT Community

Keeping Up with Crypto

What the new encryption standards mean for your business

Dec 10, 2019

Today's Speakers

Ben Yarbrough
CEO
Calyptix Security

Lawrence Teo
Founder & VP of
Development

Agenda

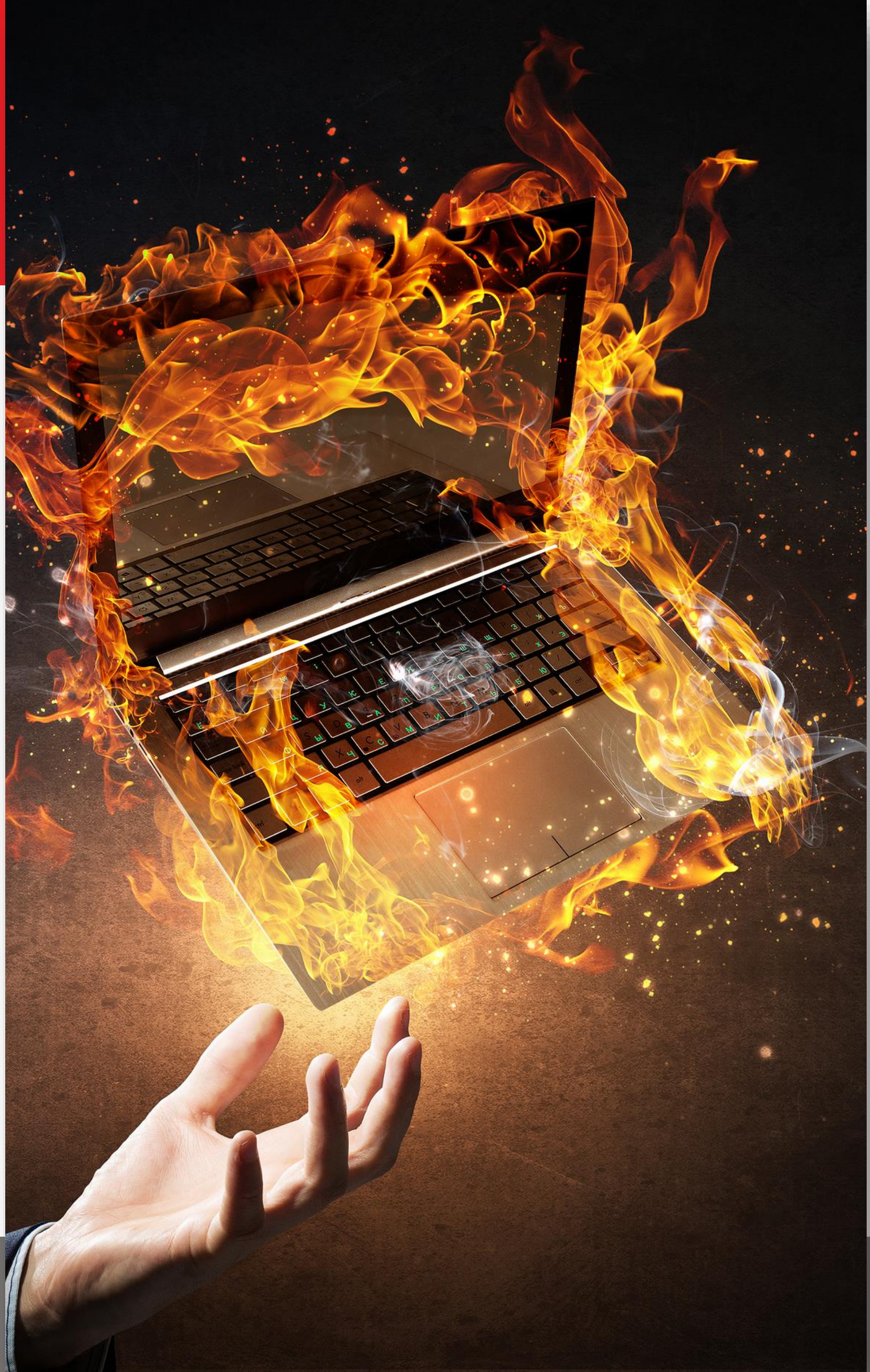
- Huge cost of bad crypto
- What is cryptography?
- Emerging trends
- Common mistakes
- Calyptix and crypto

Huge Cost of Crypto Mistakes

calyptix®
SECURITY

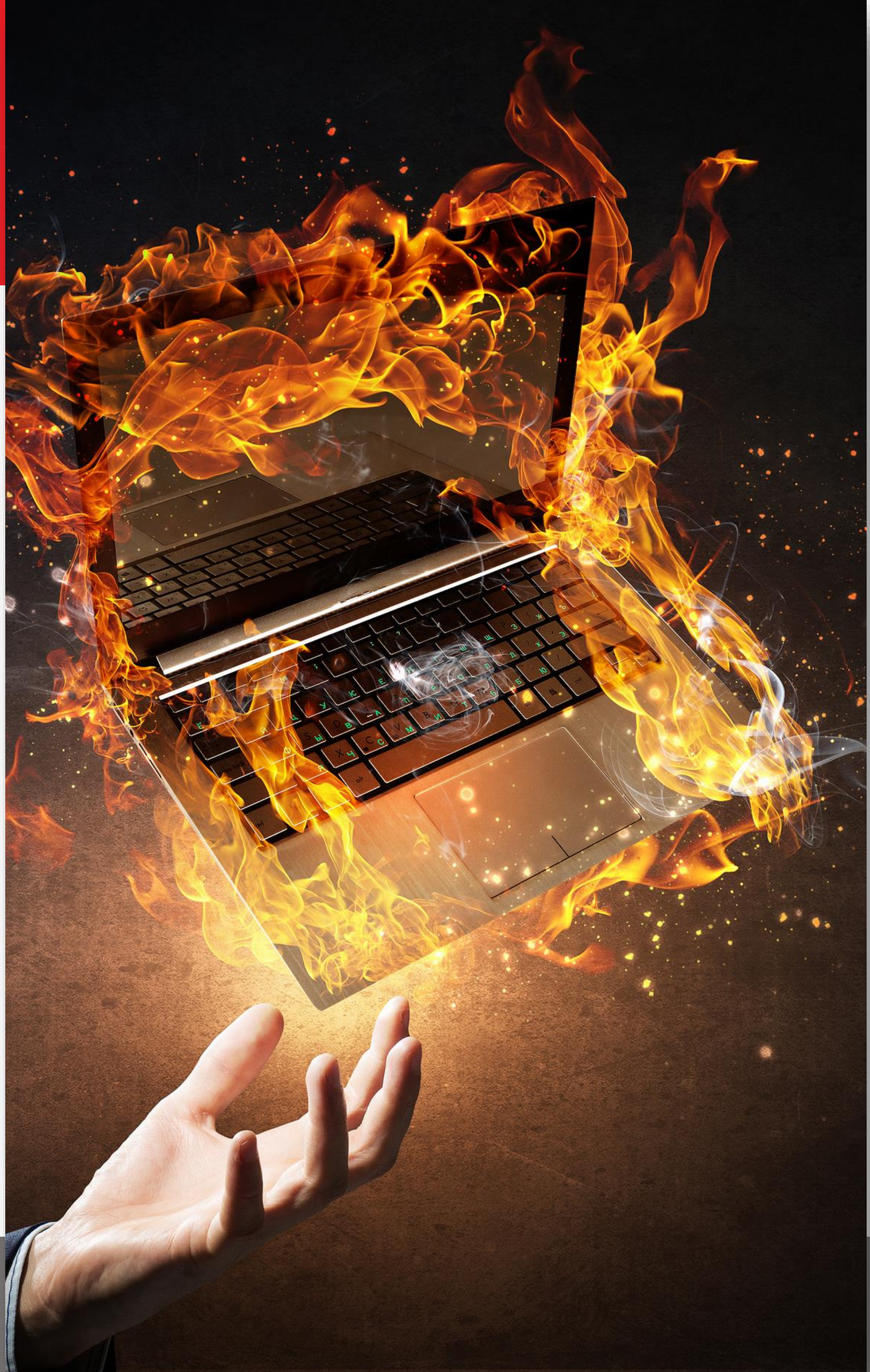
Facebook – Mar 2019

- Stored 200 – 600 million user passwords in plain text on internal server
- Searchable by thousands of employees
- No abuse discovered



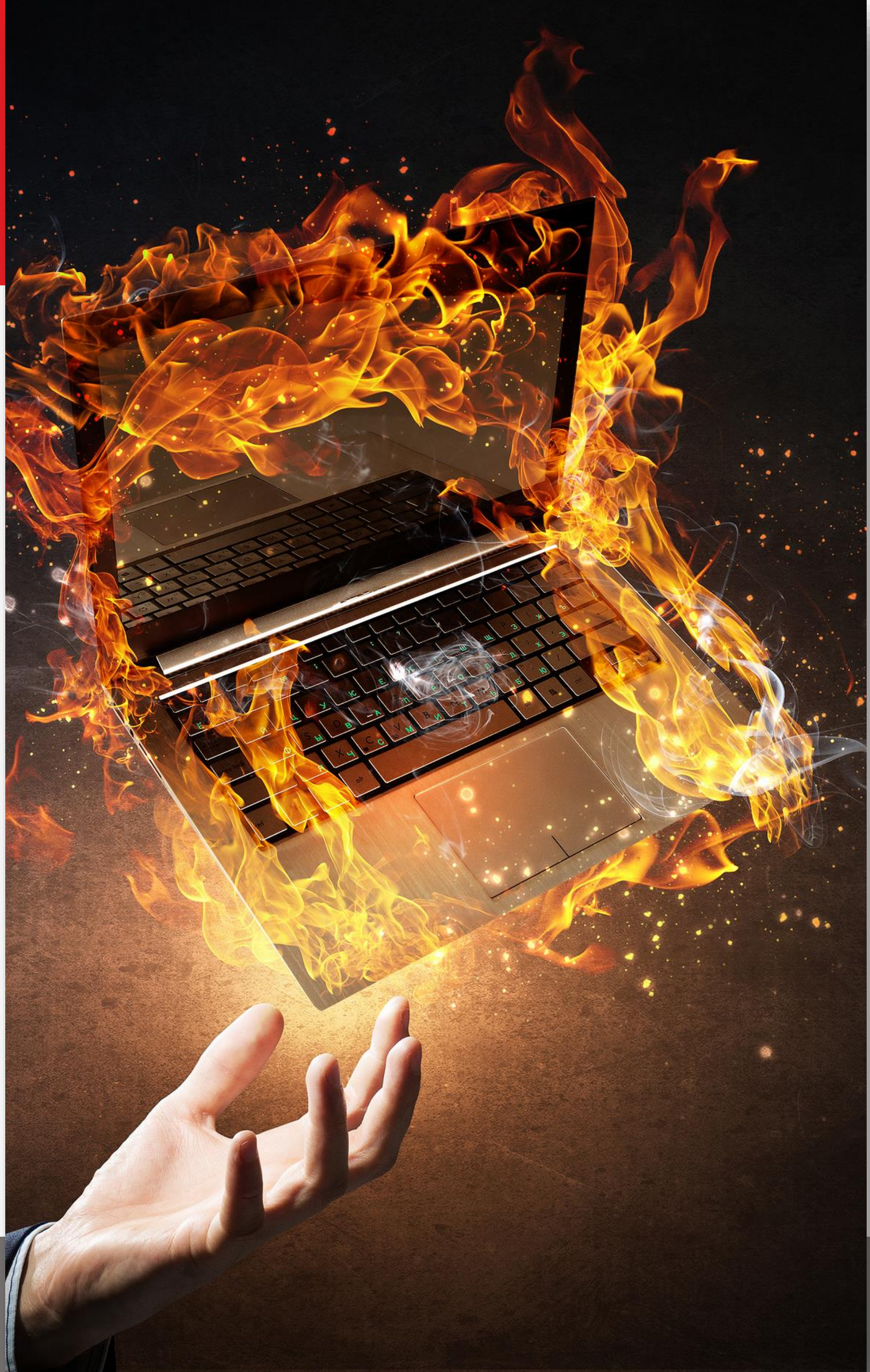
Sony PS3 – Jan 2011

- Researchers cracked PS3 and revealed keys used to load software on to the machine
- Caused by failure to generate a different random number for each signature
- Hackers cracked the key using “simple algebra”



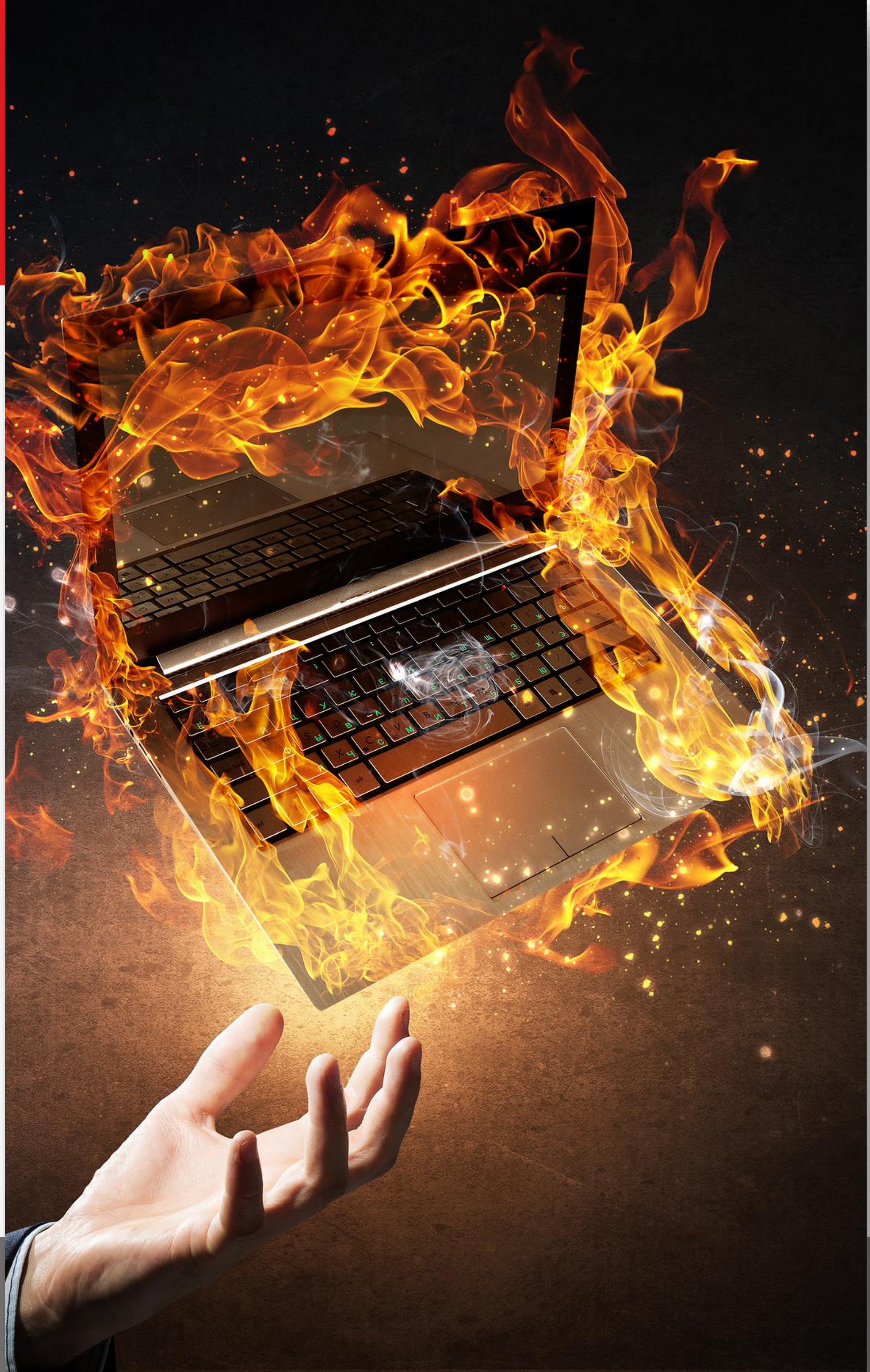
Dropbox - Aug 2016

- 68 million credentials stolen
- Roughly half stored with weak encryption
- Password reset for millions of customers



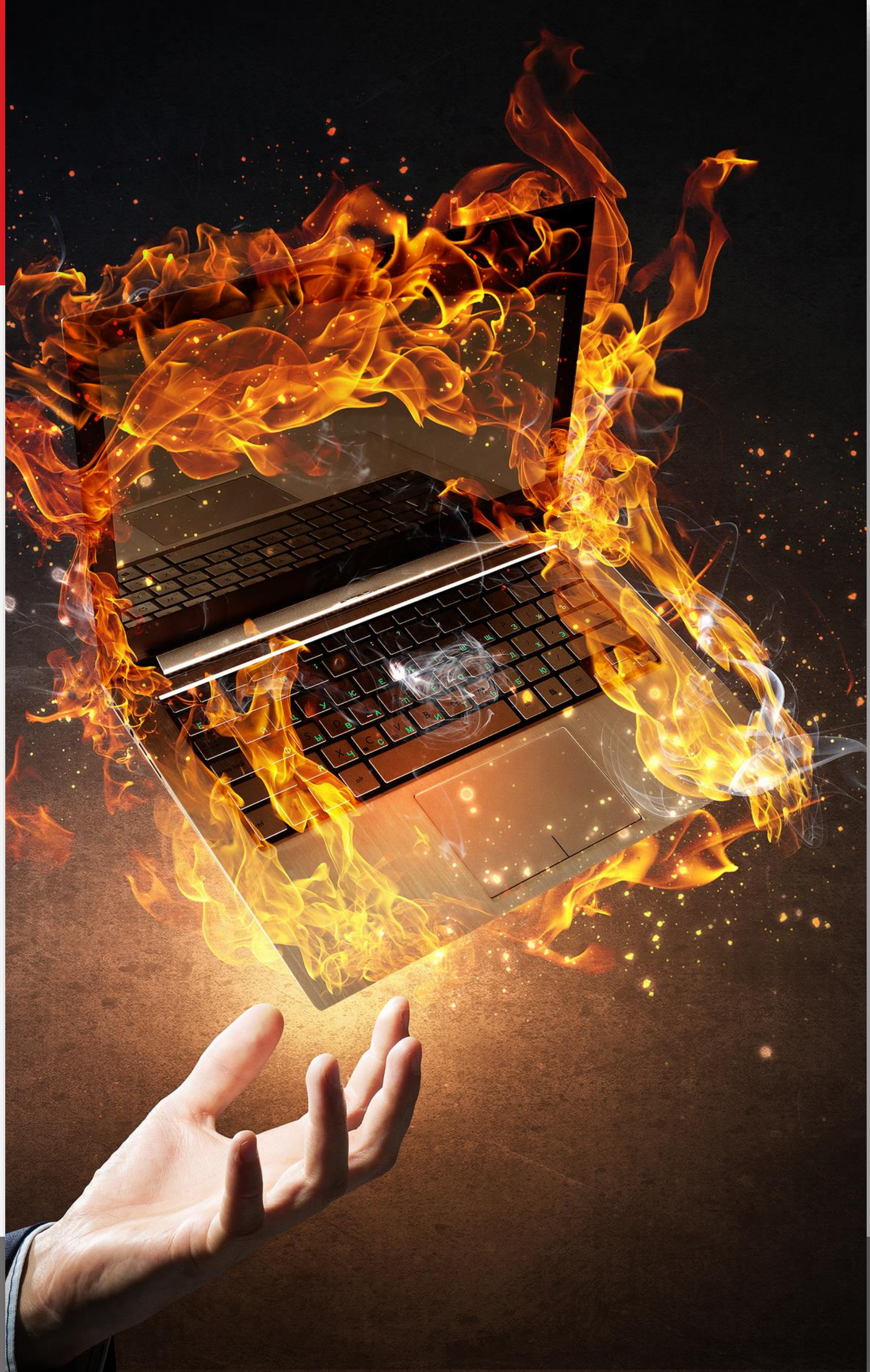
Flame – May 2012

- Malware used for espionage in the Middle East
- Malicious code signed using a fraudulent copy of a Microsoft certificate that used the weak MD5 hash algo

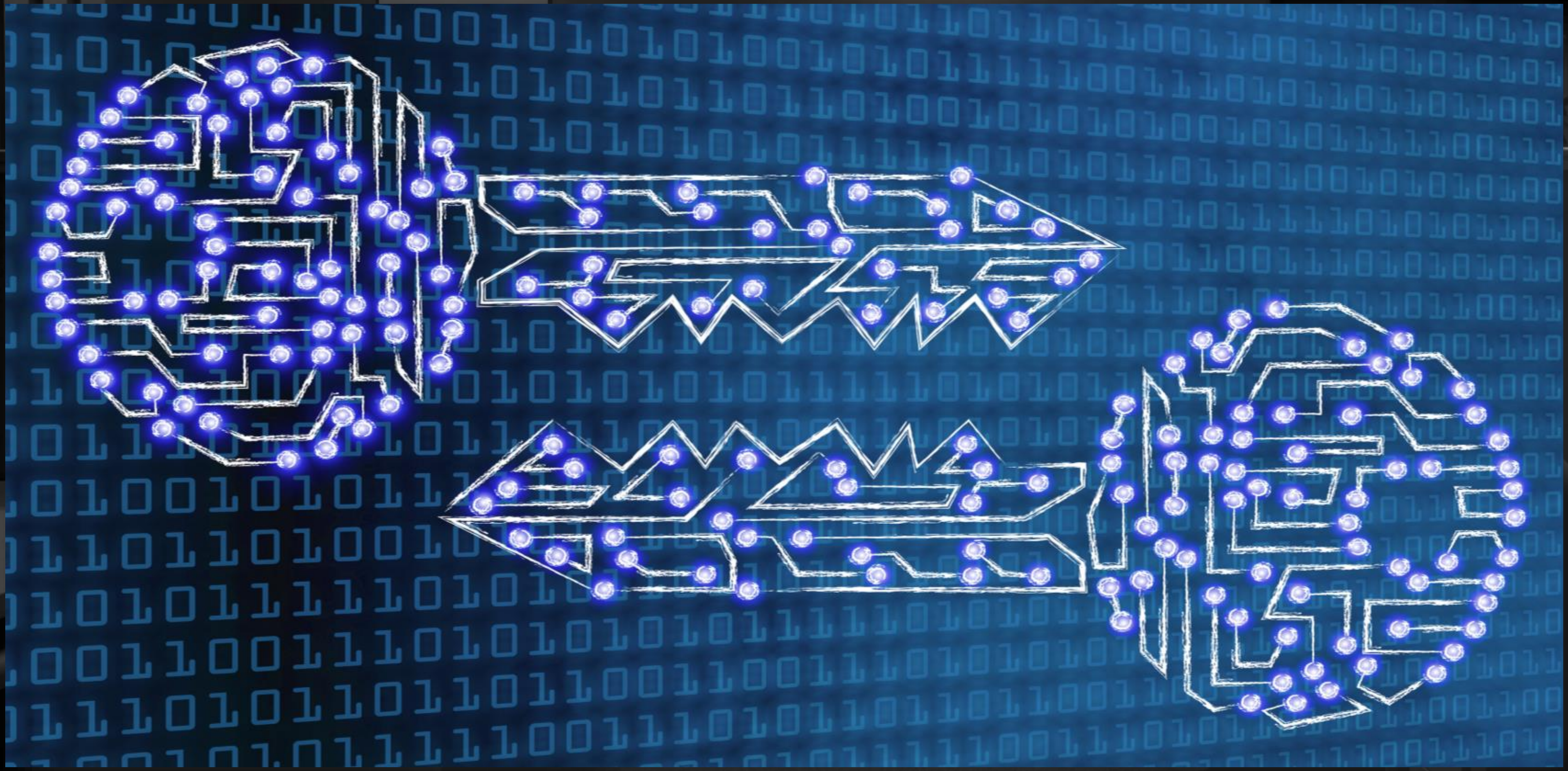


Fortinet – Nov 2019

- A weak encryption cipher (XOR) and hardcoded cryptographic keys used for communication protocols
- Left users vulnerable to eavesdropping and manipulated server responses for 18 months

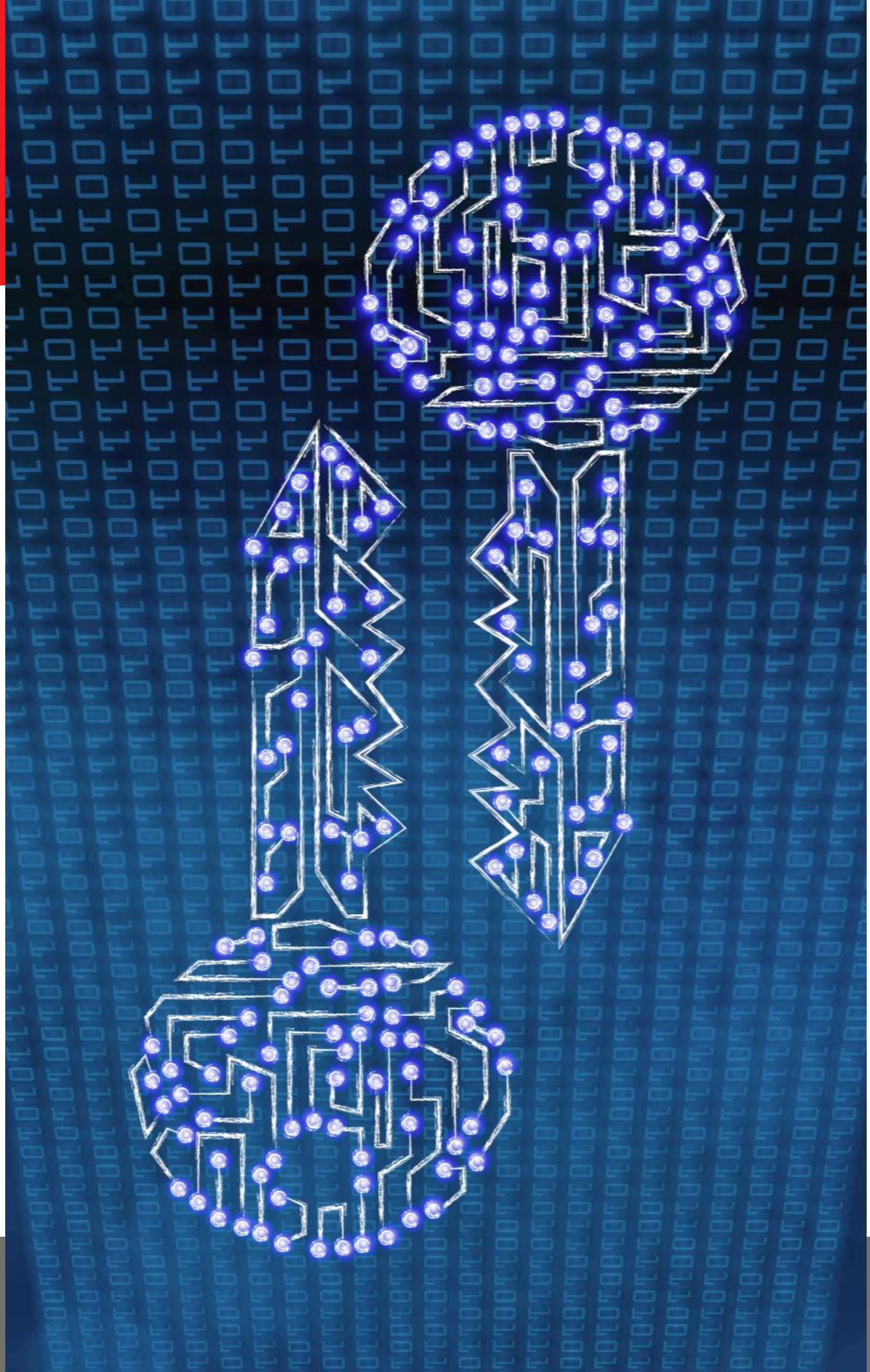


What is Cryptography?



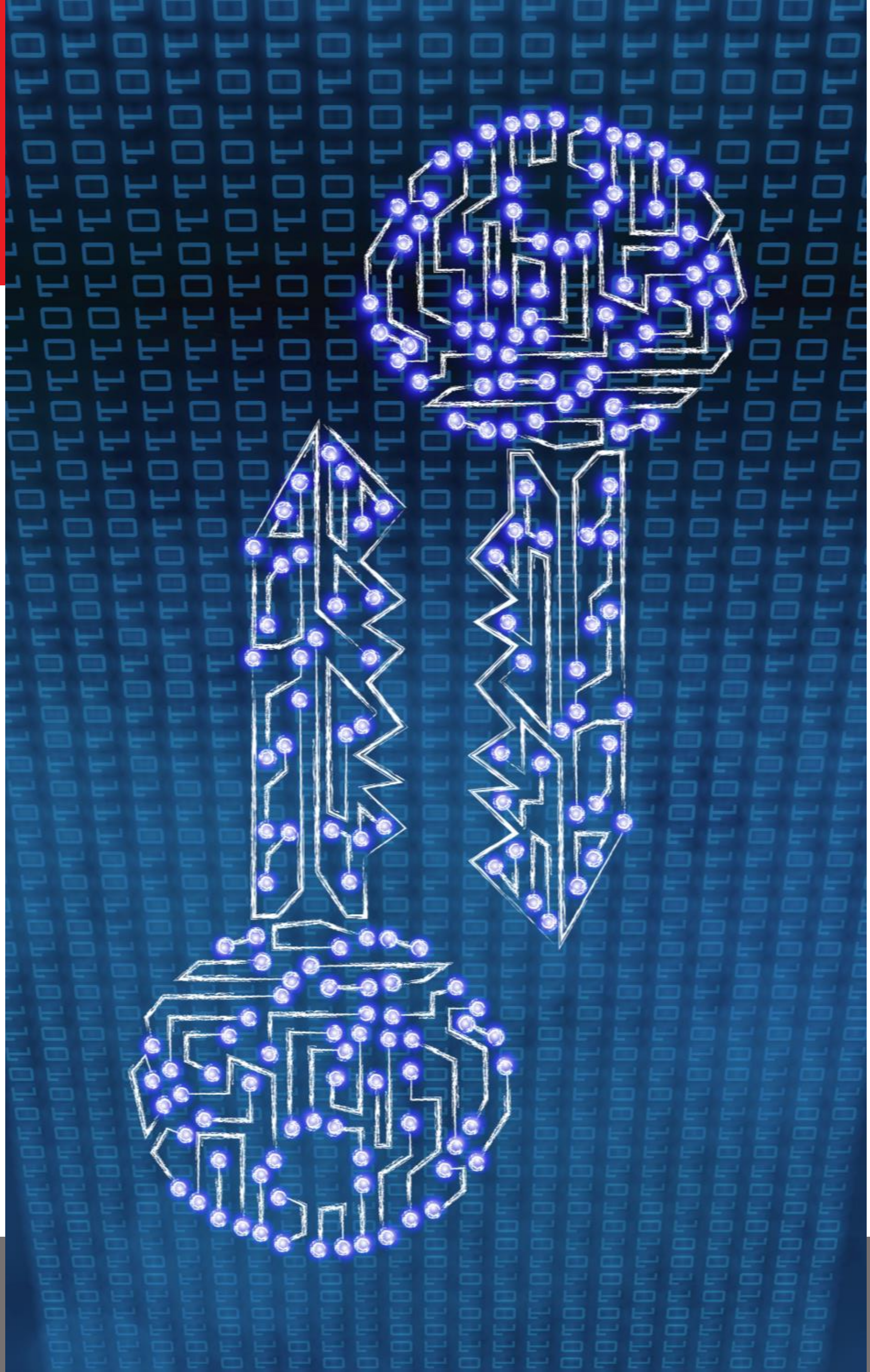
Cryptography

- Means of secure communication
- Supports two parts of security triad
  - Confidentiality
  - Integrity
  - Availability



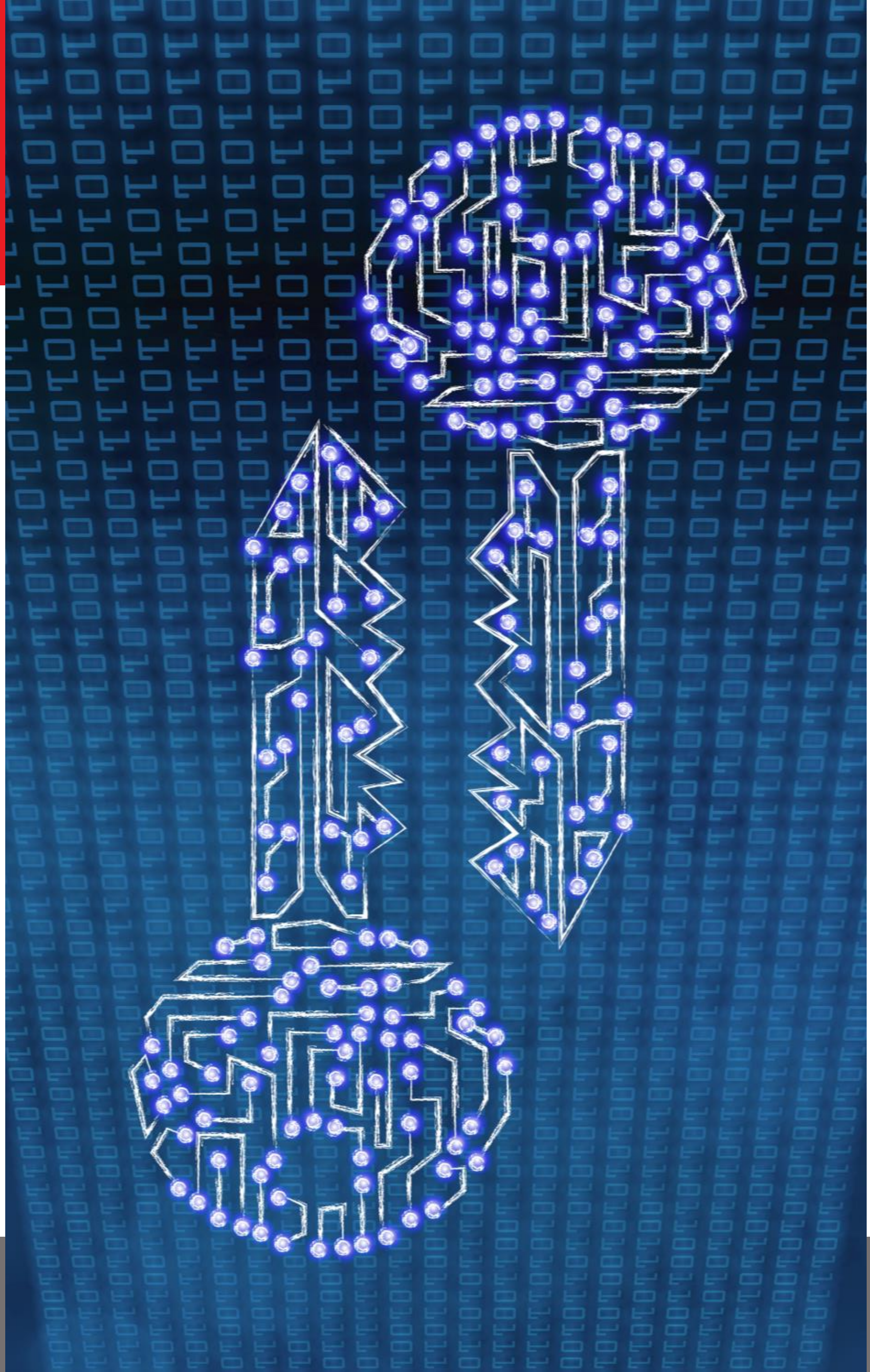
Cryptography

- Three types we'll cover
  - Symmetric key
  - Asymmetric key
  - Cryptographic hash



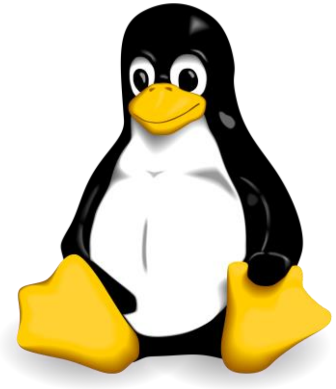
Symmetric – Block Ciphers

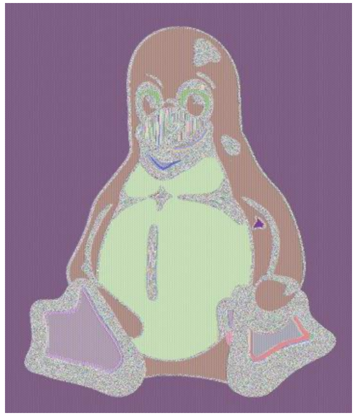
- Encrypts block-by-block (e.g. 64-bit chunks) using a key
  - Security depends on block size and key size
- Many messages are larger than 1 block and must be "chained"
  - Different ways of encrypting larger messages is known as "Modes of Operation

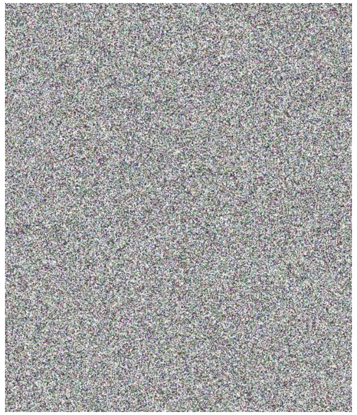


Symmetric – Block Ciphers

- Modes of Operation
  - Cipher Block Chaining (CBC) – okay
  - Counter Mode (CTR) – good
  - Electronic Code Book (ECB) – bad!
    - You can see the penguin

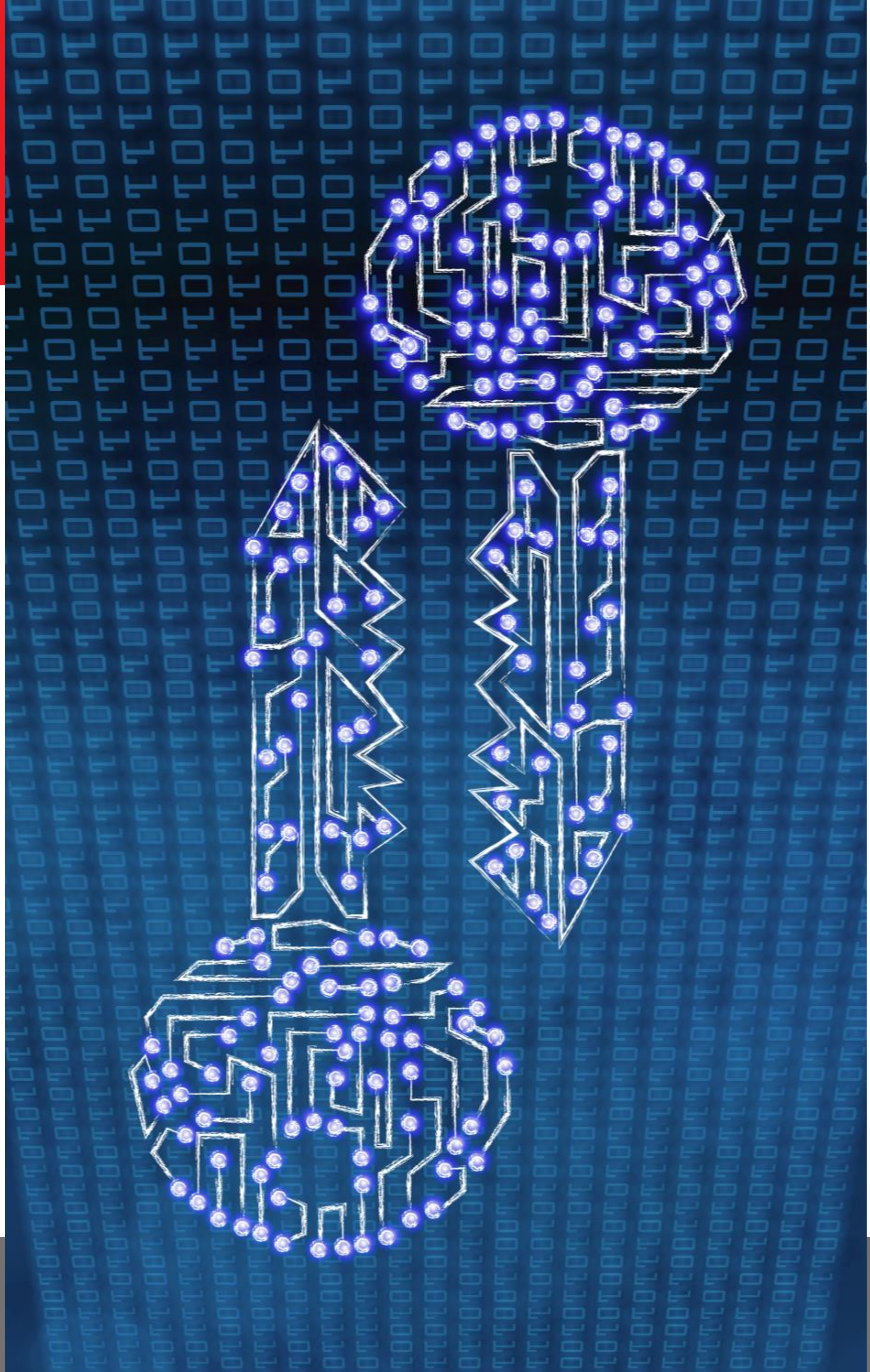






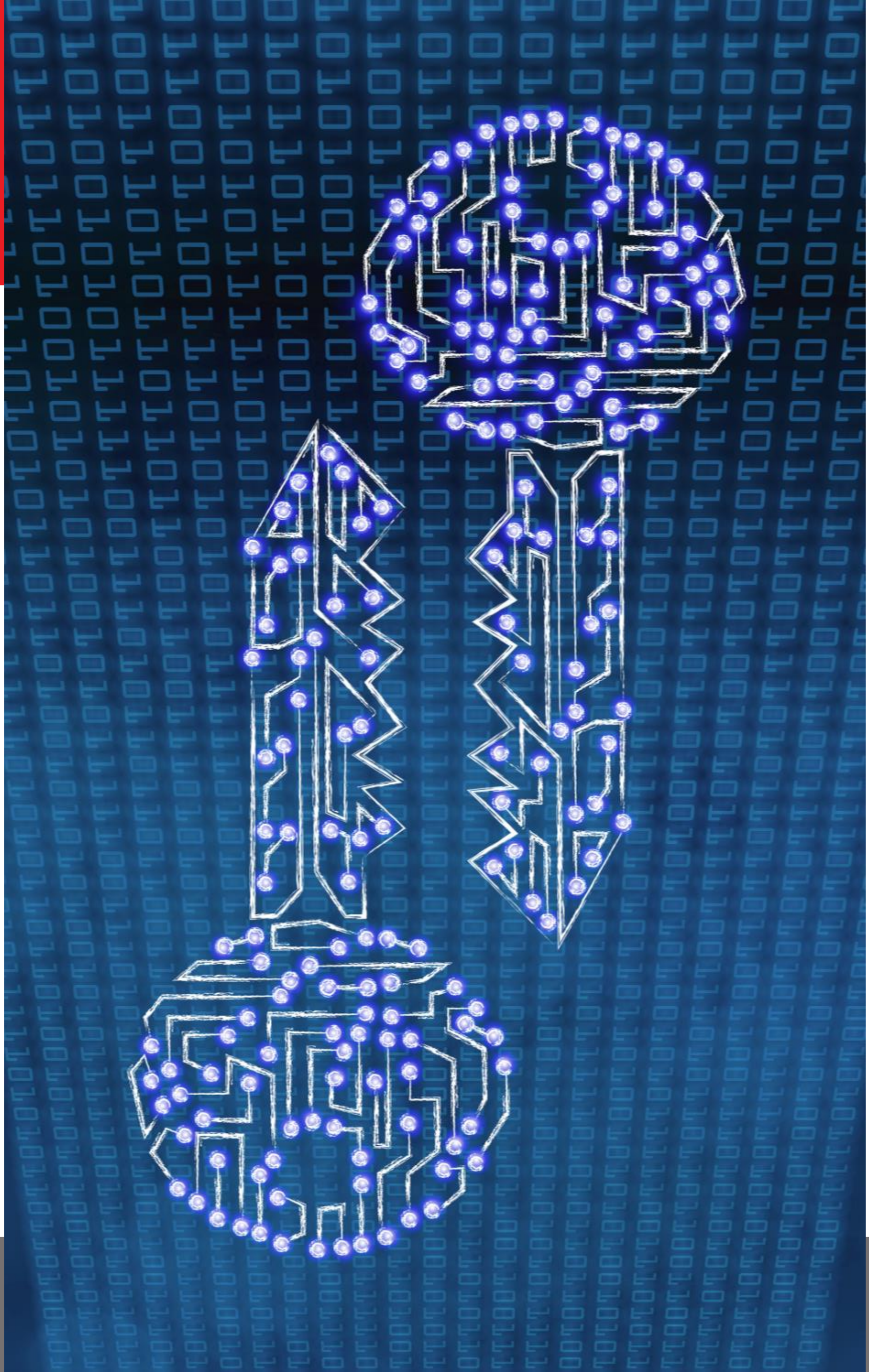
Symmetric – Stream Ciphers

- Used to encrypt streams of data
- Common ciphers
  - ChaCha20
  - Salsa20
  - RC4 – never use!



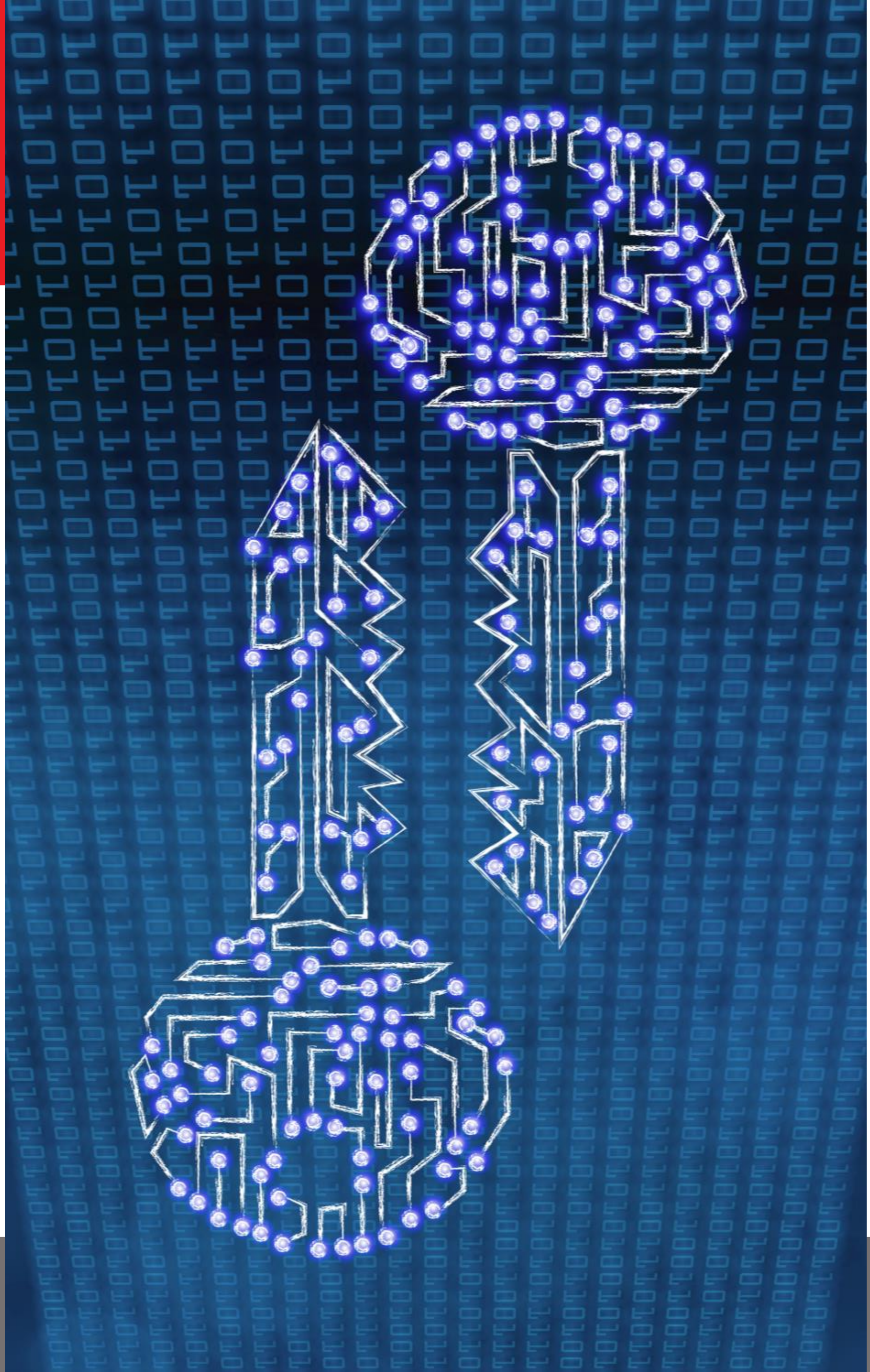
Asymmetric Key

- Aka “public key” encryption
- Three examples
  - RSA: Integer Refactorization
  - Diffie-Hellman: Discrete Logarithm
  - Elliptic Curve



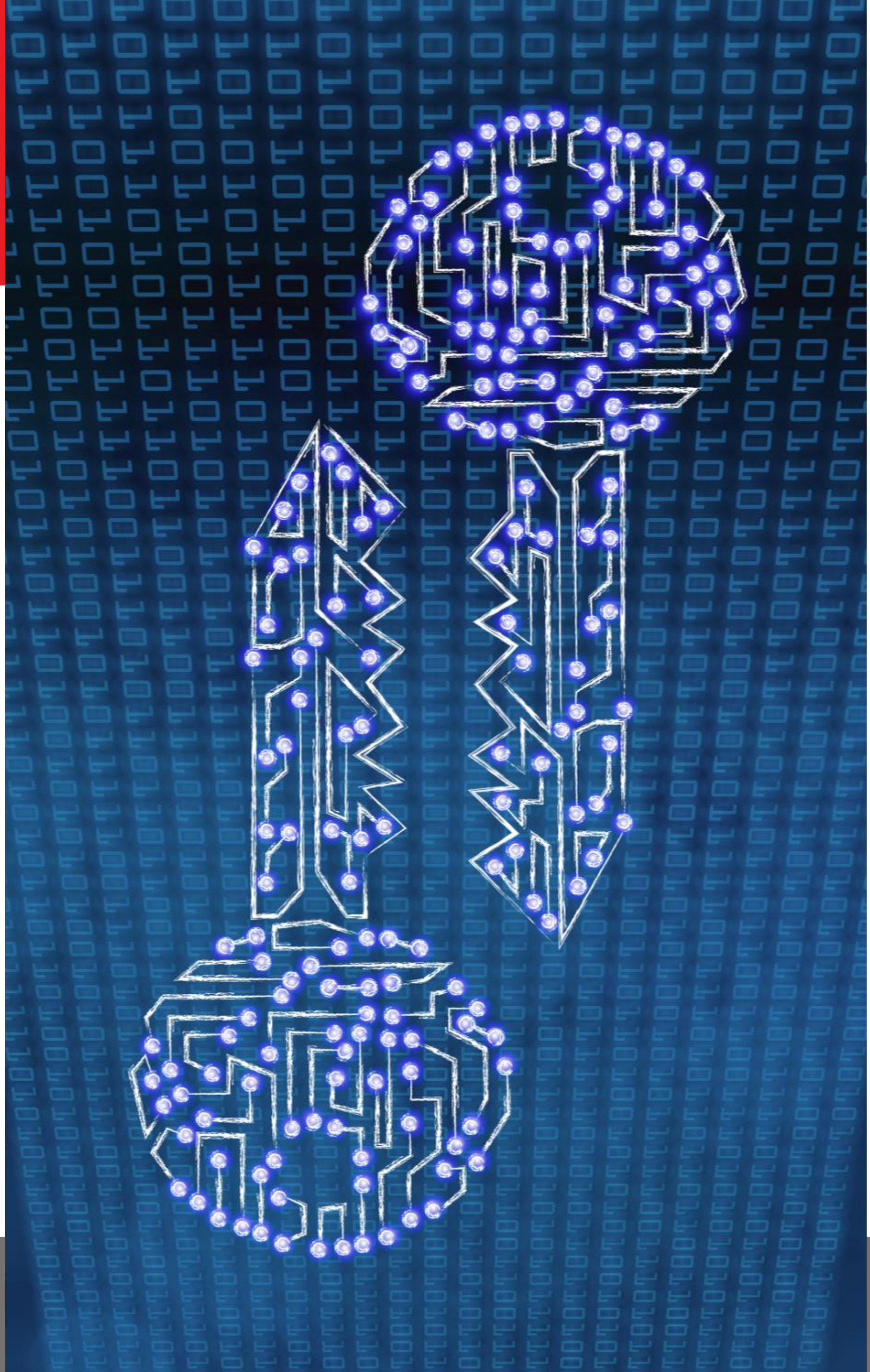
Crypto Hash Algorithm

- Equation used to convert data into encrypted output
- Properties
  - One-way hashes
  - Not reversable
  - Resistant to collisions
- Widely used in digital signatures / certificates



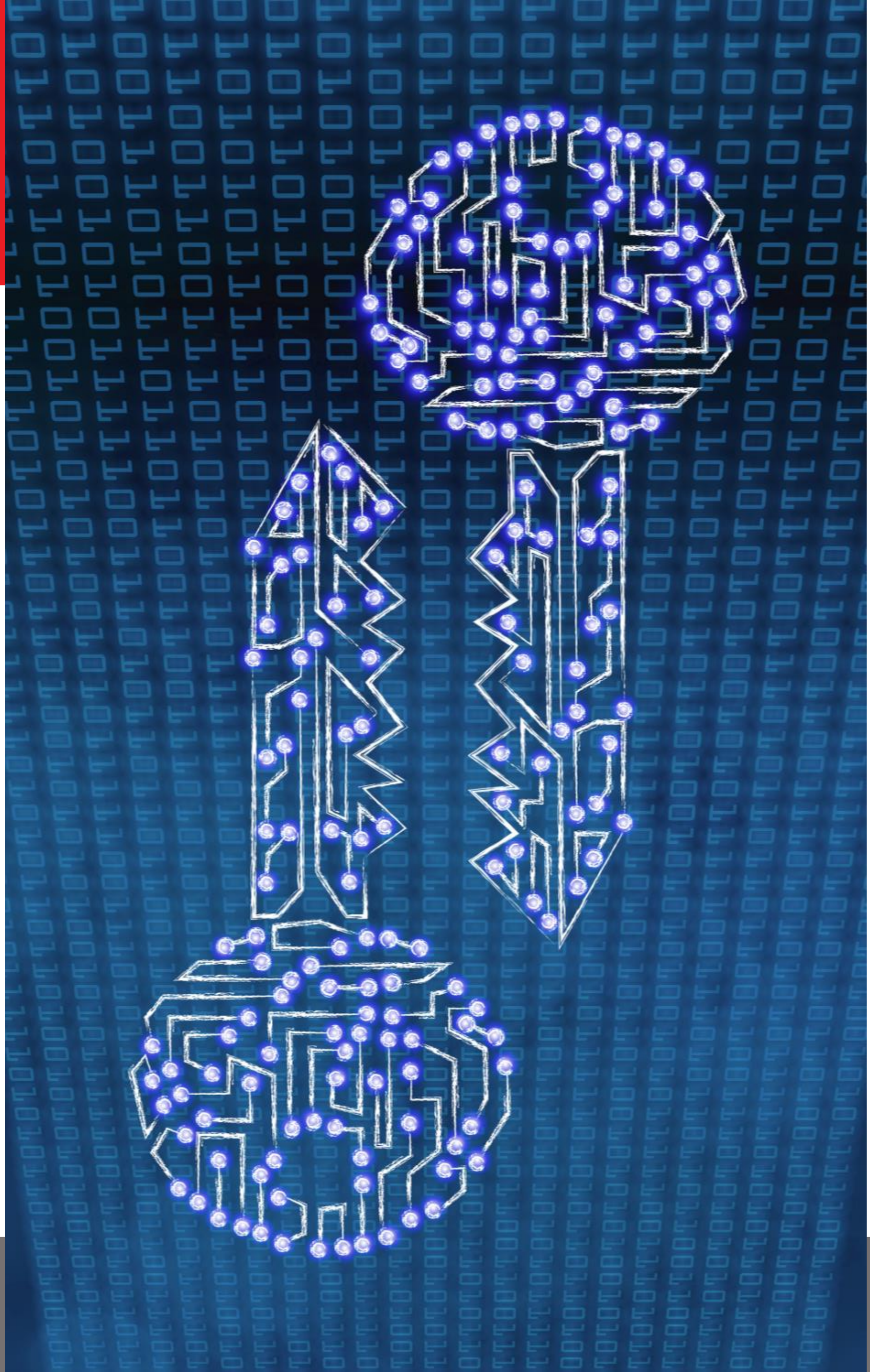
Crypto Hash Algorithm

- Examples
  - MD5 – do not use!
  - SHA-1 – do not use!
  - SHA-2
    - SHA-256, SHA-384, SHA-512
  - SHA-3



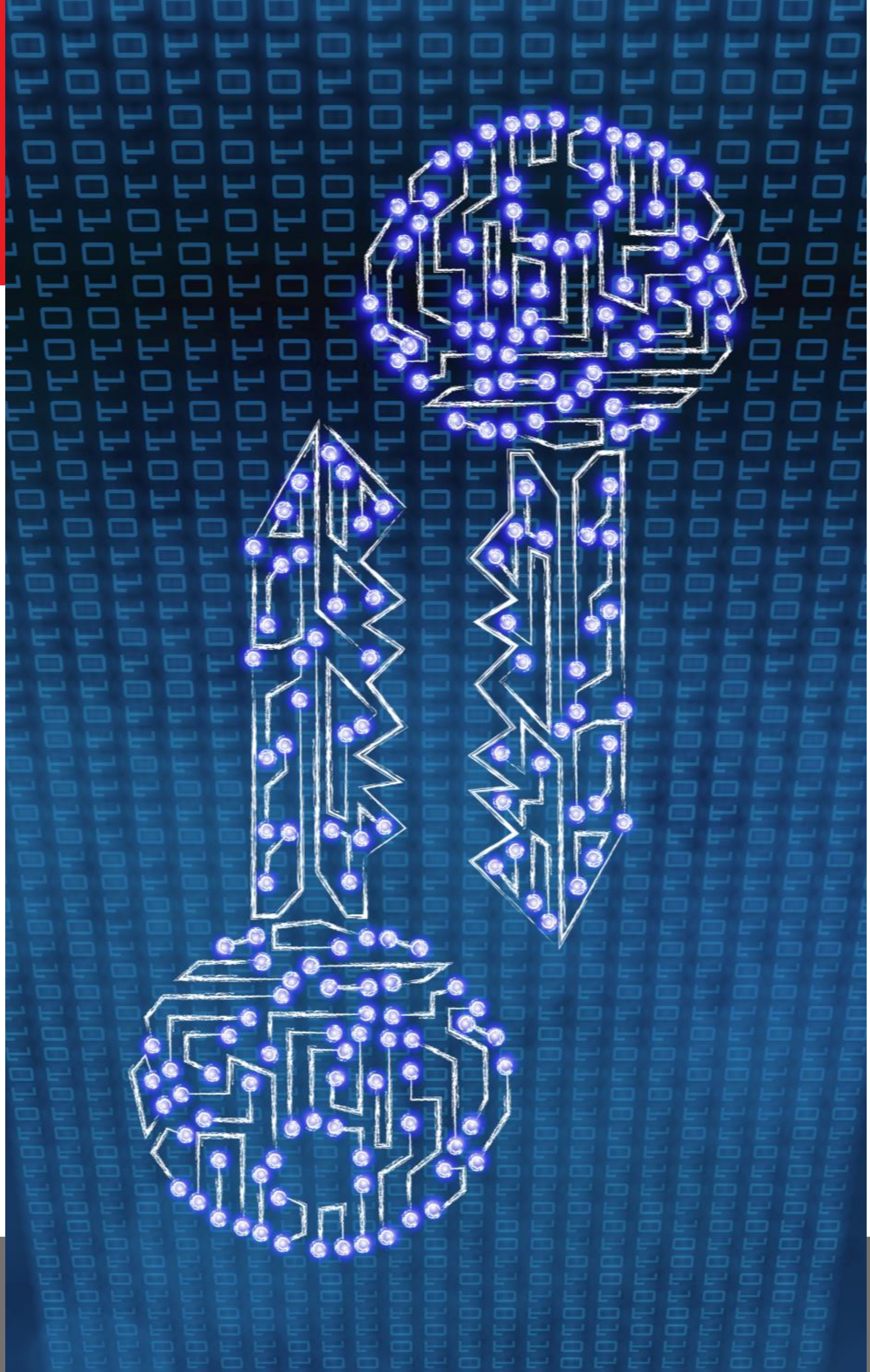
Other Crypto Topics

- Key derivation functions
- Message authentication codes (MACs)
- Authenticated encrypted modes



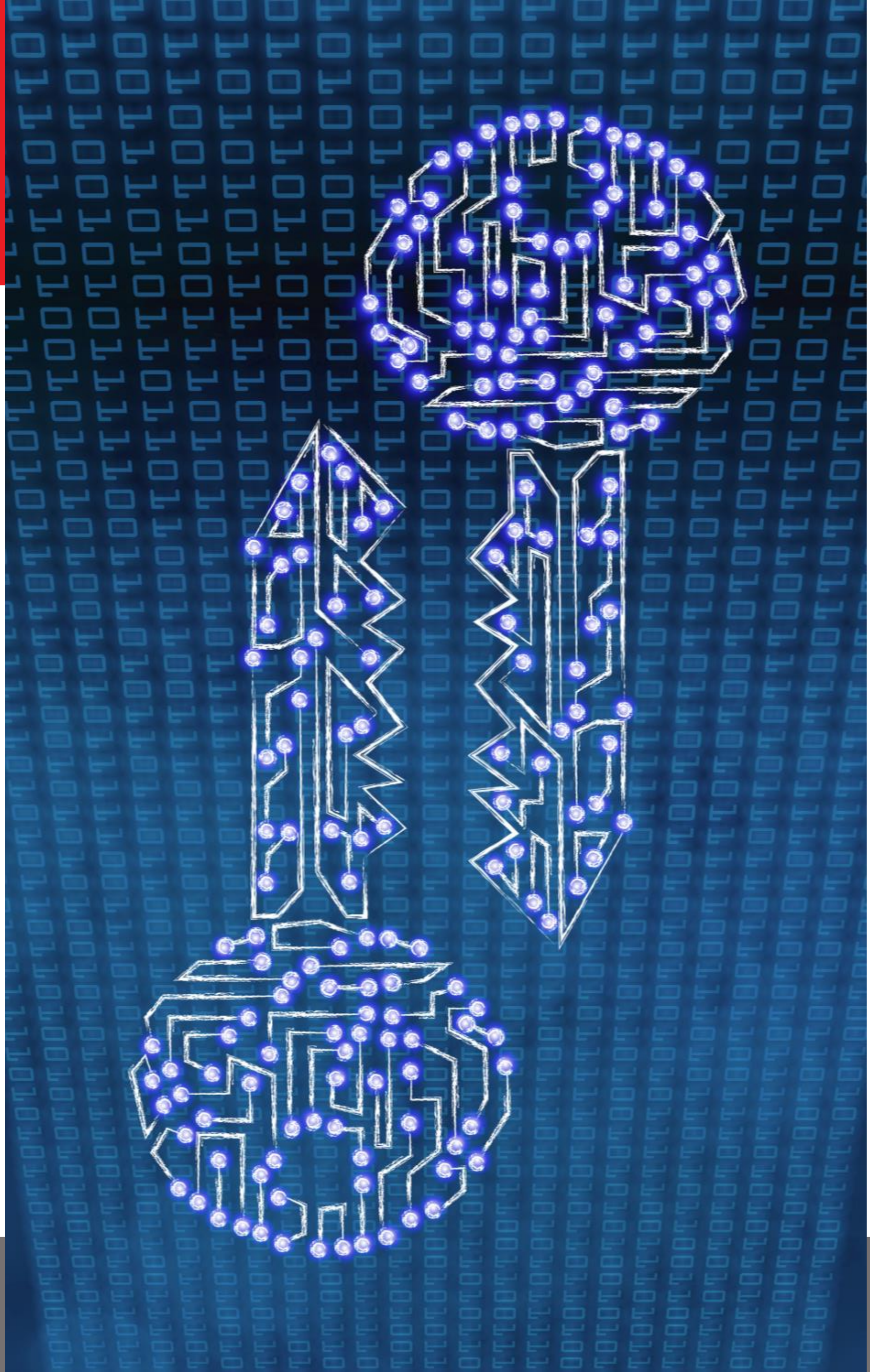
Crypto in Networks

- VPN
- Backup systems
- Wireless
- Credit card processing
- RDP
- HTTPS

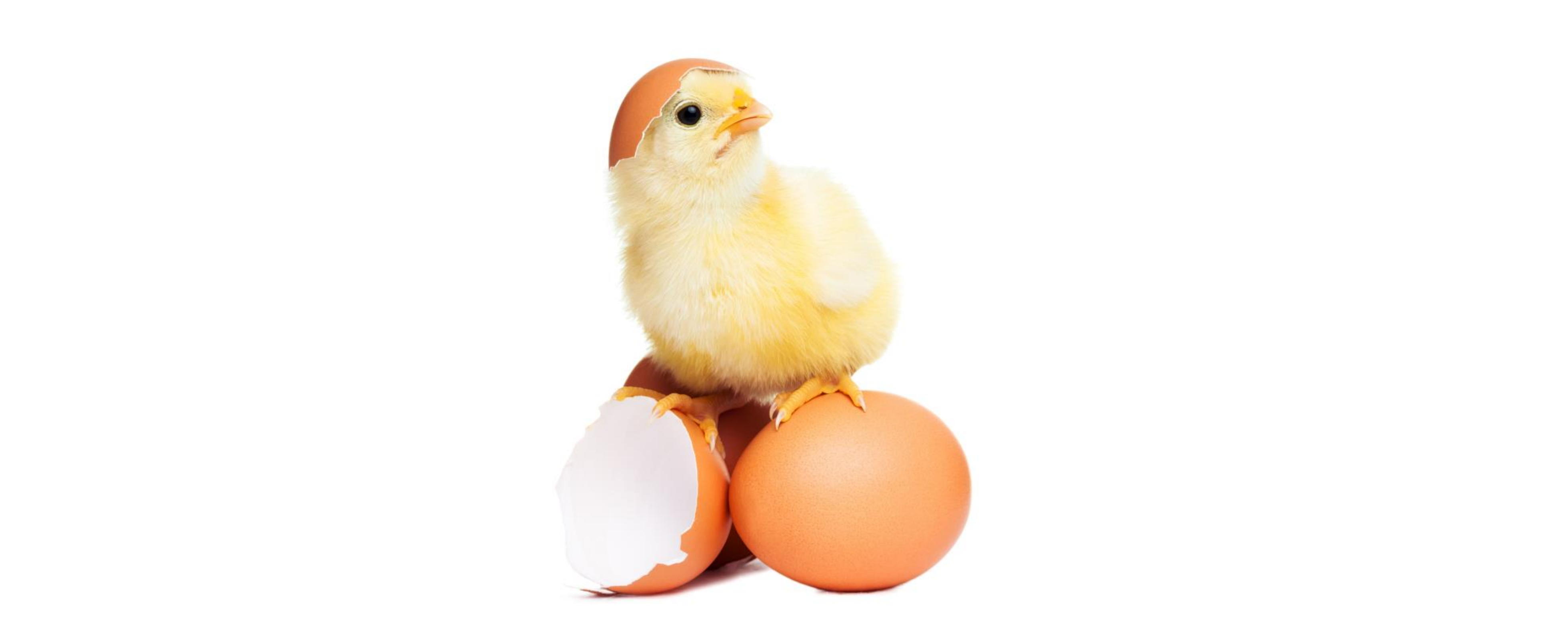


HTTPS Example

- Website identity verified by certificate
  - Crypto hash algorithms
- Establish session key
  - Asymmetric cryptography
- Data encrypted using session key
  - Symmetric cryptography



Emerging Trends



calyptix®
SECURITY

HTTPS Everywhere

- HTTPS adoption accelerated in 2015
- More than half of all webpages loaded by Chrome are via HTTPS
- Great news for security
- Harder to monitor user web activity

HTTPS MITM

- Some security products break HTTPS encryption to inspect traffic
  - Known as HTTPS inspection, HTTPS web filtering, TLS filtering, etc.
- This is an intentional man-in-the-middle (MITM) "attack"
- Product can see all HTTPS traffic in plain text

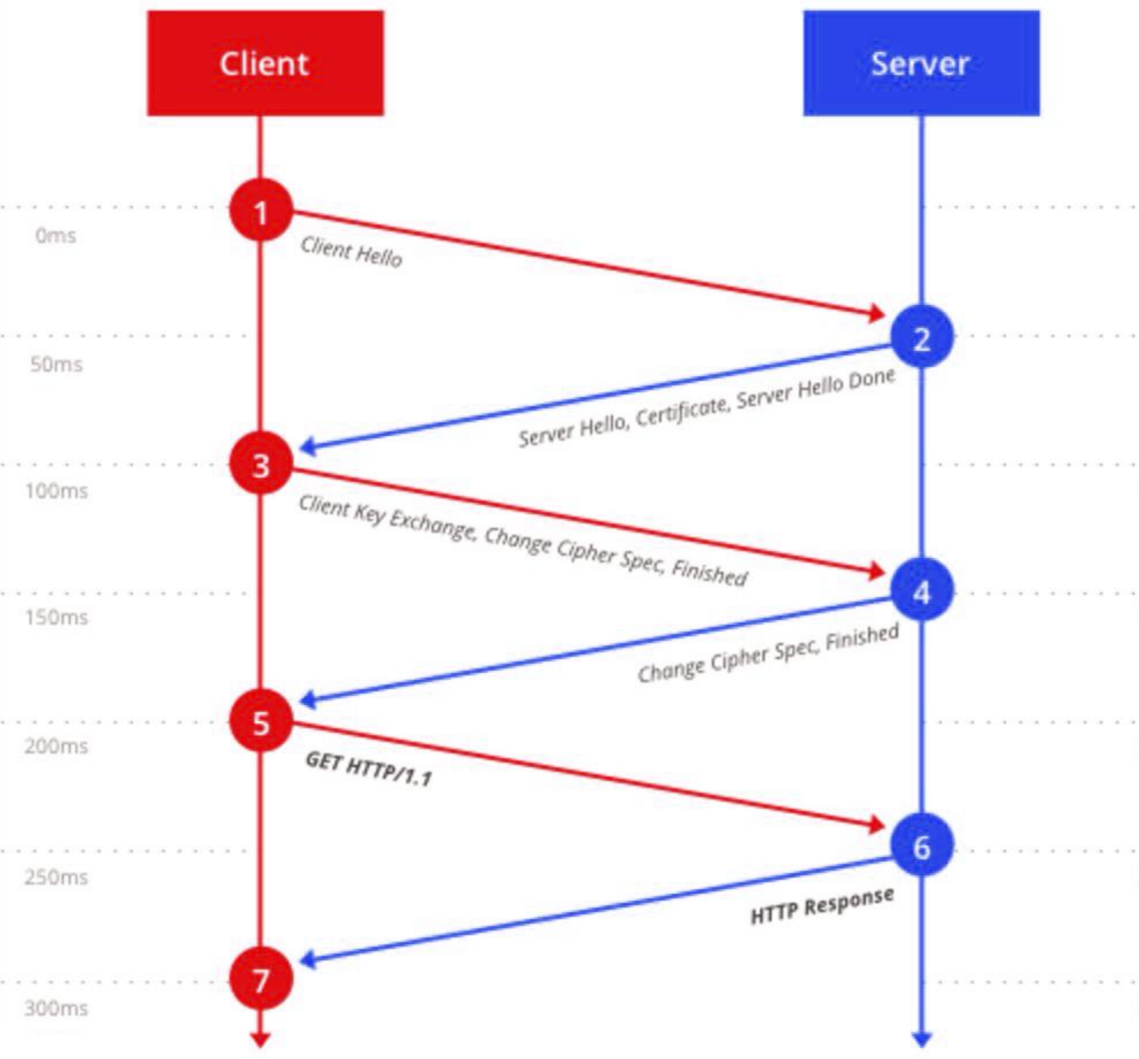
HTTPS MITM

- Risks associated
  - Research shows many of the products negatively impact connection security
  - Product vulnerabilities could unintentionally modify transactions
  - Service becomes potential attack target
- Discouraged by CERT, NSA, and other security researchers

TLS 1.3

- TLS 1.2 is considered secure
  - Depends on configuration
- TLS 1.3 aims
  - Encrypt more of the negotiation packets
  - Remove support for weak algo’s
  - Forward secrecy by default
  - Improved performance

TLS 1.2 *(Full Handshake)*



Client

Server

1 *Client Hello*

2 *Server Hello, Certificate, Server Hello Done*

3 *Client Key Exchange, Change Cipher Spec, Finished*

4 *Change Cipher Spec, Finished*

5 ***GET HTTP/1.1***

6 ***HTTP Response***

7

0ms

50ms

100ms

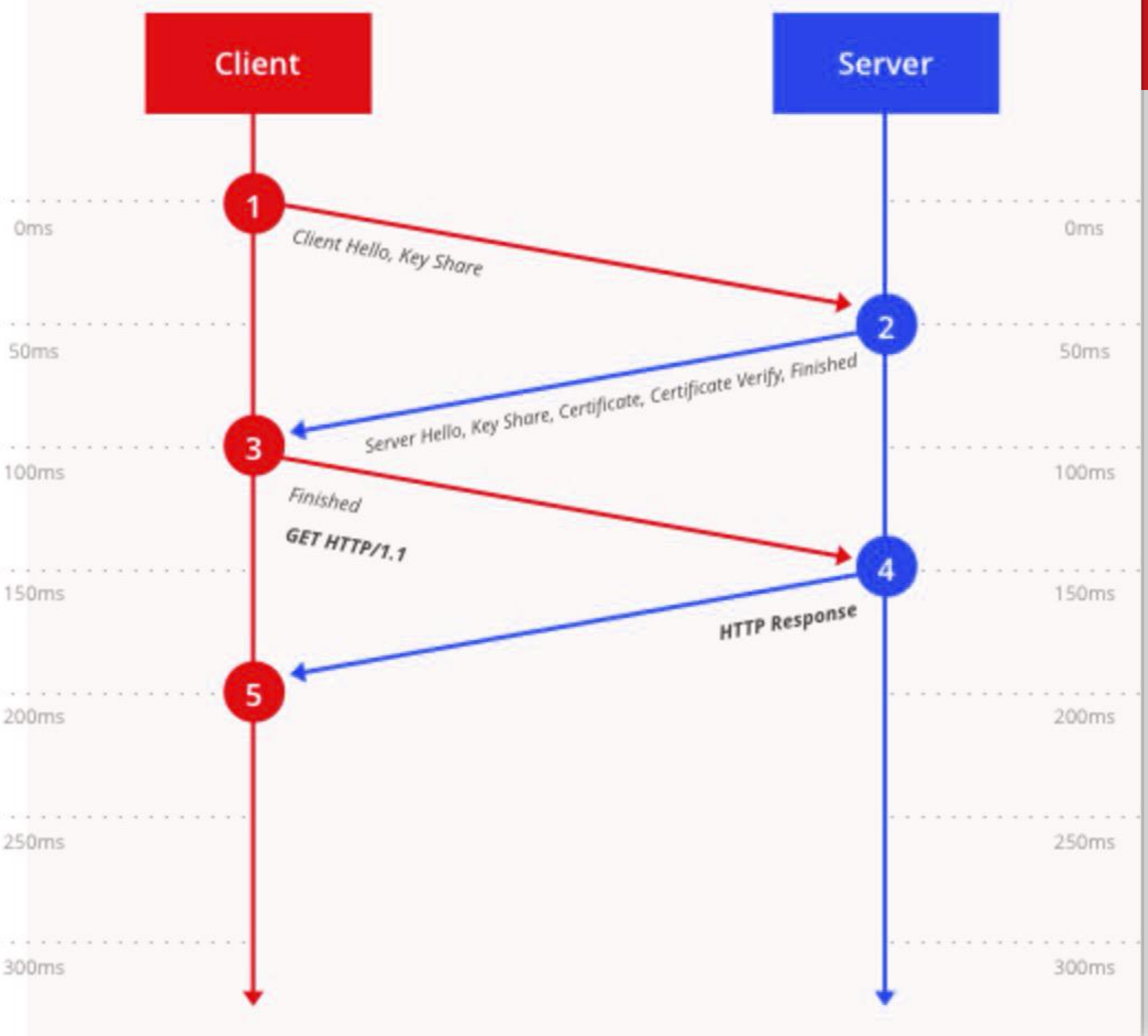
150ms

200ms

250ms

300ms

TLS 1.3 *(Full Handshake)*



Client

Server

1 *Client Hello, Key Share*

2 *Server Hello, Key Share, Certificate, Certificate Verify, Finished*

3 *Finished*

GET HTTP/1.1

4 ***HTTP Response***

5

0ms

50ms

100ms

150ms

200ms

250ms

300ms

Encrypted SNI

- TLS shows server name via Server Name Indication (SNI) extension
- Encrypted SNI is an OPTIONAL extension for TLS 1.3
- Still a (rapidly evolving) draft
- Latest implementation:
  - Publish the Encrypted SNI configuration (public key + metadata) via a new DNS resource record called HTTPSSVC (HTTPS Services)

DNS Over HTTPS

- Attempts to encrypt all DNS queries
  - Even query to retrieve encrypted SNI configuration
- Currently a standard (RFC 8484) although implementation details are still being worked out

DNS Over HTTPS

- Other DNS security technologies
  - DNSCrypt
  - DNS Over TLS
  - DNSSEC
- DNS Over HTTPS is more likely to see adoption
  - Pushed by Cloudflare and Mozilla

Mistakes in Cryptography

calyptix®
SECURITY

Not using crypto

- Unencrypted passwords
  - Leaving them in a plain-text doc
- Unencrypted VoIP
  - Almost never secured properly
- Credit card transaction over HTTP

Weak password

- Strong cryptography cannot protect information secured with the password “123456”

Choosing Obsolete Crypt.

- Never use
  - DES, MD5, SHA1
  - SSL v3.0, TLS 1.0
  - Diffie-Hellman parameters less than 2048-bits
  - Unsalted hashes for passwords
- When to check
  - Configuring crypto (such as with IPsec VPN tunnel)
  - Choosing vendors (ask for their crypto details)

Insecure Mode of Op.

- Never use Electronic Code Block (ECB)
- Use CBC correctly
  - Always randomize IV

Choosing Bad Implement.

- Avoid flawed operating systems
- Bad pseudo random number generator (PRNG)

Failure to Protect Keys

- Common mistake
  - Storing keys together with encrypted data
  - Always store separately in secure environment

Making Your Own Crypto

- Always use industry-standard, peer-reviewed cryptographic technology
- Never use in-house algorithms

Assuming Compliance = Good Crypto

- Network security regulations (such as PCI DSS) set a baseline
- Always strive to be more secure than “minimum”

About Us

calyptix®
SECURITY

AccessEnforcer UTM Firewall

- ✓ Intrusion prevention
- ✓ Web filter
- ✓ Unlimited VPN
- ✓ VLAN
- ✓ LAN Lockdown
- ✓ Multi-WAN
- ✓ Bandwidth mgt. (QoS)
- ✓ Automatic updates

calyptix® SECURITY

Keep Up with Crypto

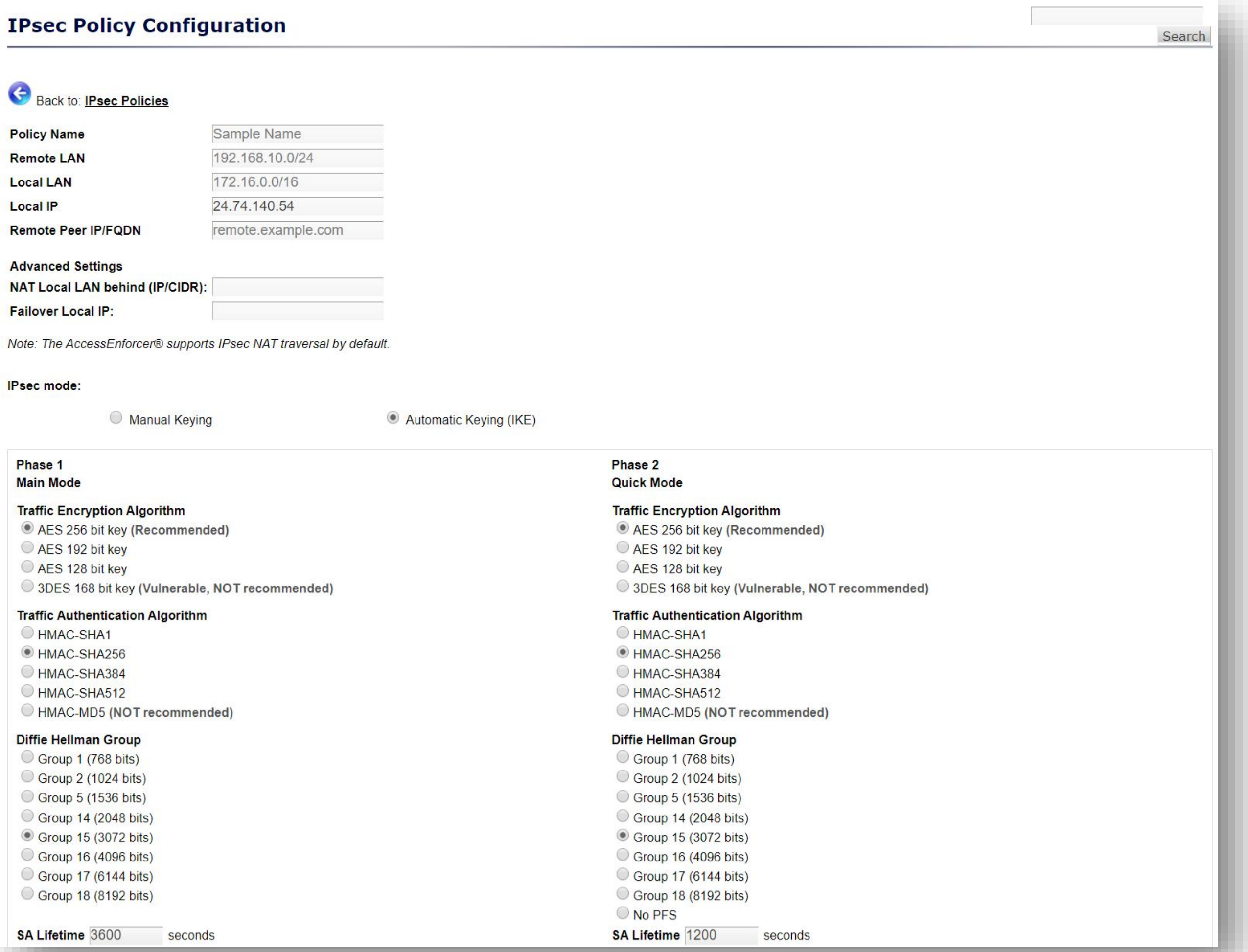
- Passwords
  - Unique password for every device
  - Encrypted with bcrypt
  - Soon to use Argon2
- Web GUI
  - Accessible only via HTTPS (TLS 1.2+)

Keep Up with Crypto

- Automatic updates
  - TLS-based
  - Uses client and server authenticated (not just server auth.)
  - Download encrypted with AES256
- 4096-bit Diffie-Hellman params.
  - For web GUI and CalyptixVPN

Keep Up with Crypto

- IPsec VPN page
  - Recommends secure algos.
  - Warns against broken algos.



IPsec Policy Configuration

Back to: IPsec Policies

Policy Name	Sample Name
Remote LAN	192.168.10.0/24
Local LAN	172.16.0.0/16
Local IP	24.74.140.54
Remote Peer IP/FQDN	remote.example.com

Advanced Settings

NAT Local LAN behind (IP/CIDR):

Failover Local IP:

Note: The AccessEnforcer® supports IPsec NAT traversal by default.

IPsec mode:

○ Manual Keying ● Automatic Keying (IKE)

Phase 1
Main Mode

Traffic Encryption Algorithm
● AES 256 bit key (Recommended)
○ AES 192 bit key
○ AES 128 bit key
○ 3DES 168 bit key (Vulnerable, NOT recommended)

Traffic Authentication Algorithm
○ HMAC-SHA1
● HMAC-SHA256
○ HMAC-SHA384
○ HMAC-SHA512
○ HMAC-MD5 (NOT recommended)

Diffie Hellman Group
○ Group 1 (768 bits)
○ Group 2 (1024 bits)
○ Group 5 (1536 bits)
○ Group 14 (2048 bits)
● Group 15 (3072 bits)
○ Group 16 (4096 bits)
○ Group 17 (6144 bits)
○ Group 18 (8192 bits)

SA Lifetime 3600 seconds

Phase 2
Quick Mode

Traffic Encryption Algorithm
● AES 256 bit key (Recommended)
○ AES 192 bit key
○ AES 128 bit key
○ 3DES 168 bit key (Vulnerable, NOT recommended)

Traffic Authentication Algorithm
○ HMAC-SHA1
● HMAC-SHA256
○ HMAC-SHA384
○ HMAC-SHA512
○ HMAC-MD5 (NOT recommended)

Diffie Hellman Group
○ Group 1 (768 bits)
○ Group 2 (1024 bits)
○ Group 5 (1536 bits)
○ Group 14 (2048 bits)
● Group 15 (3072 bits)
○ Group 16 (4096 bits)
○ Group 17 (6144 bits)
○ Group 18 (8192 bits)
○ No PFS

SA Lifetime 1200 seconds

Keep Up with Crypto

- CalyptixVPN
  - Encrypts and authenticates all control channel packets
  - 2048-bit RSA certs signed with SHA256
  - AES-256-GCM for encryption
  - SHA256 for authentication
  - Uses PRNG from LibreSSL
    - Which uses OpenBSD's ChaCha20-based PRNG
  - Unique 4096-bit Diffie Hellman parameters for every AccessEnforcer
    - Params. are generated on a bare metal OpenBSD system (not subject to entropy issues from VMs or hypervisors)

Keep Up with Crypto

- LibreSSL
- Auto-updated OpenSSH
- OpenBSD operating system
  - Very secure OS with strong PRNG system to support crypto features
- All updated automatically

Firewall Case Study

- Charlotte-area marketing firm
- 30 AccessEnforcer devices
- First device deployed
  - Jan 7. 2012

Firewall Case Study

- **May 19, 2014:** v3.1.15.52
  - CalyptixVPN SSL certs. upgraded to 2048-bit.
- **Oct 14, 2014:** v3.1.15.73
  - SSL v3.0 disabled on HTTPS GUI
- **Oct 31, 2014:** v3.1.16.156
  - HTTPS GUI switched from OpenSSL to LibreSSL
  - HTTPS GUI Enforces high ciphers and excludes MD5 and RC4.
  - HTTPS GUI accepts TLS v1.1 and TLS v1.2.
- **Apr 9, 2015:** v3.1.16.210
  - Generated SSL certs and CSRs are signed using SHA256 (in preparation for the deprecation of SHA1 certs).
  - Removed RSA 512-bit and RSA 1024-bit key size options for Generated SSL certs and CSRs
- **Jun 24, 2015:** v3.1.17.102
  - TLS v1.0 is disabled by default on the web interface for new AccessEnforcer units.
  - Existing units will preserve existing behavior (TLSv1.0 is enabled).
  - The TLS v1.0 setting can be enabled or disabled
  - Default SSL certificate for GUI uses SHA256 as its signature algorithm on new units.
  - GUI and CalyptixVPN use unique 4096-bit Diffie Hellman groups for key exchange. (Logjam)
  - New units have locally generated CalyptixVPN certs. SHA256 as signature algorithm.

Firewall Case Study

- **Oct 17, 2016:** v3.64.20.54
  - CalyptixVPN updated to use OpenVPN 2.3.12.
  - CalyptixVPN session key renegotiated after every 64MB of data (Sweet32 Vulnerability)
  - Blowfish removed from the IPsec VPN GUI (Sweet32 Vulnerability).
  - 3DES marked as "Vulnerable, NOT recommended" on the IPsec VPN GUI. Popup warning appears if enabled.
  - AES-256 is now the default and recommended algorithm for IPsec VPN.
- **Mar 3, 2017:** v3.64.21.34
  - Removed support for the obsolete SSH1 key.
  - Disabled all 3DES cipher suites from being used to serve the HTTPS GUI to counter the Sweet32 vulnerability.
- **Oct 24, 2017:** v4.0.2 Build 369
  - CalyptixVPN updated to use OpenVPN 2.4.4
  - CalyptixVPN estimated to be roughly 30% faster compared to the v3.64 version.
  - CalyptixVPN control channel is encrypted and is authenticated using HMAC-SHA256 instead of HMAC-SHA1.
  - Introduced CalyptixVPN Legacy Mode, which displays a banner on the GUI if your system is using legacy crypto (e.g. SHA1, 1024-bit RSA, or 64-bit Blowfish) for CalyptixVPN.
  - CalyptixVPN server uses the LibreSSL/OpenBSD pseudorandom number generator (PRNG) that is based on the strong and fast ChaCha20 cipher.

Firewall Case Study

- **Mar 19, 2018:** v4.0.4 Build 43
  - Upgraded OpenSSH to 7.6
  - Configuable IKEv2 IPsec VPN policies
  - CalyptixVPN works with OpenVPN Connect for iOS, now that OpenVPN Connect for iOS has upgraded their TLS library.
- **May 6, 2018:** v4.0.5 Build 44
  - Added support for IPsec Diffie Hellman groups 14 (2048-bit MODP), 15 (3072-bit MODP), 16 (4096-bit MODP), 17 (6144-bit MODP), and 18 (8192-bit MODP).
  - CalyptixVPN updated to use OpenVPN 2.4.6
- **Jul 17, 2018:** v4.0.6 Build 45
  - Improved PCI compliance by ensuring that no weak algorithms are used for key exchange algorithms and MACs in OpenSSH.
- **Nov 28, 2018:** V4.1.0 Build 373
  - IPsec VPN policies default to using Diffie-Hellman Group 15 (3072 bits).
- **Nov 19, 2019:** V4.1.4 Build 52
  - Upgraded OpenSSH to 8.1

Special Offer

Breakthrough Starter Pack

1. $799 for 11 AccessEnforcers
2. Up to 50 More in the Go! Plan
3. 60-Day Money Back Guarantee

See the Deal: calyptix.com/ascii

QUESTIONS?

calyptix®
SECURITY

Special Offer

Breakthrough Starter Pack

1. $799 for 11 AccessEnforcers
2. Up to 50 More in the Go! Plan
3. 60-Day Money Back Guarantee

See the Deal: calyptix.com/ascii