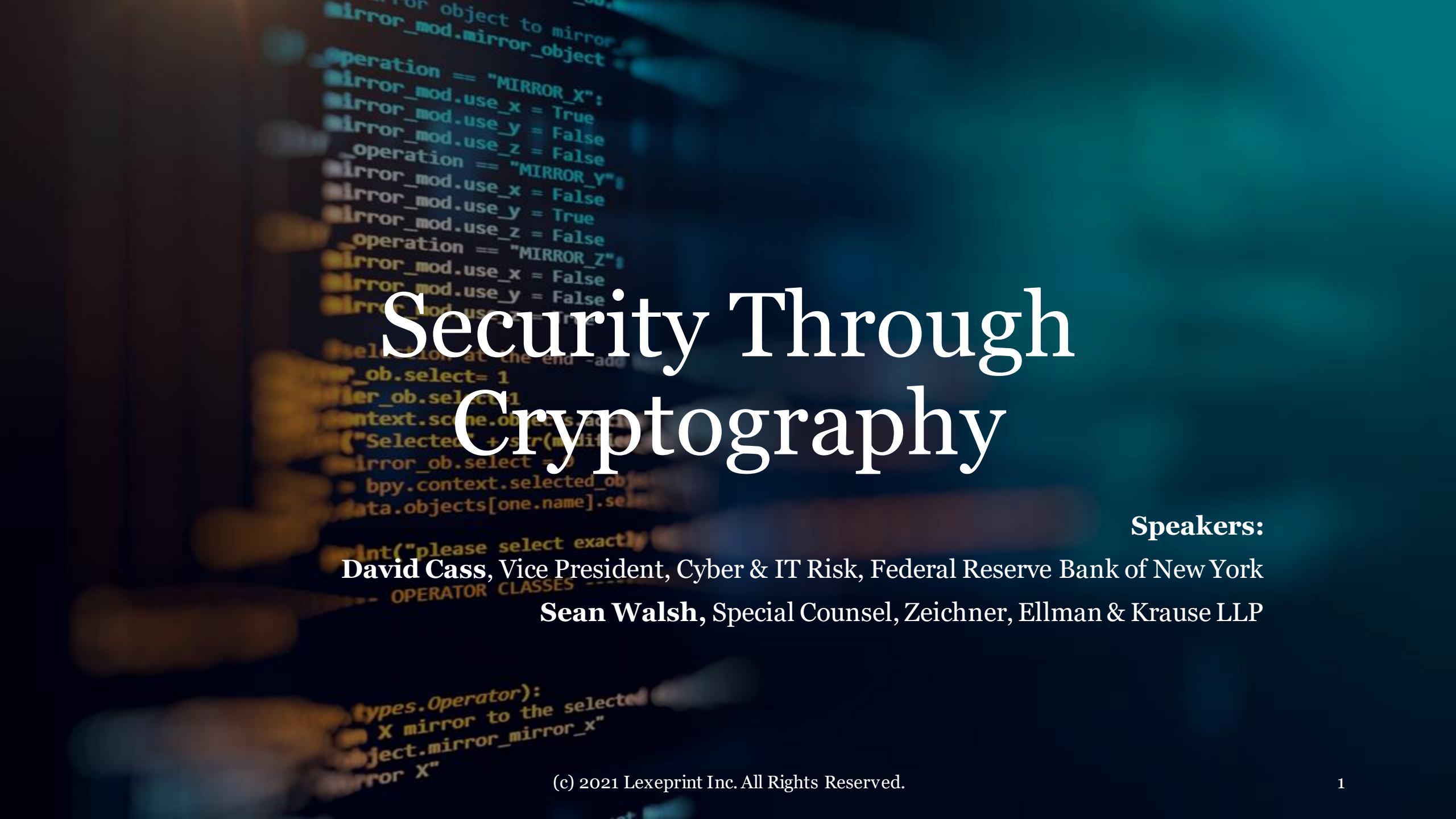


Security Through Cryptography

Speakers:

David Cass, Vice President, Cyber & IT Risk, Federal Reserve Bank of New York

Sean Walsh, Special Counsel, Zeichner, Ellman & Krause LLP

(c) 2021 Lexeprint Inc. All Rights Reserved.

Disclaimer

- This is not legal advice nor should it be considered legal advice.
- This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients.
- This presentation is offered for educational and informational uses only.

(c) 2021 Lexeprint Inc. All Rights Reserved.

Speakers



David Cass
Vice President, Cyber & IT Risk
Federal Reserve Bank of New York



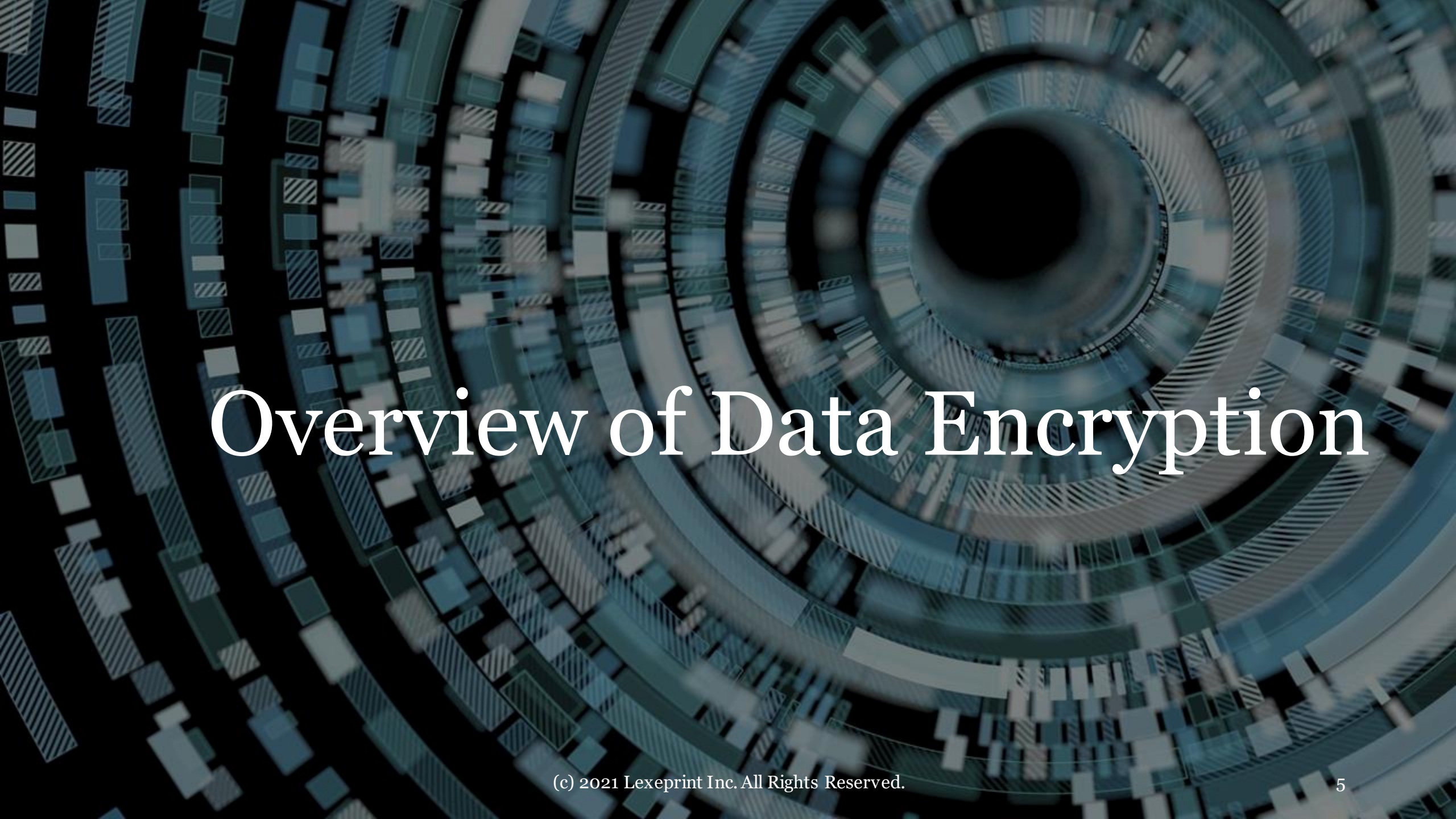
Sean Walsh
Special Counsel, Zeichner,
Ellman & Krause LLP

(c) 2021 Lexeprint Inc. All Rights Reserved.

Agenda

- Overview of Data Encryption
- Common Types of Encryption
- Asymmetric vs. Symmetric Encryption
- Key Management Lifecycle
- New Encryption Rules
- Recent Trends in Cryptography

(c) 2021 Lexeprint Inc. All Rights Reserved.



Overview of Data Encryption

(c) 2021 Lexeprint Inc. All Rights Reserved.



What is Data Encryption?

- Data encryption turns data into another form, or code, so that only people with access to a secret key or password can read it.
- Encryption is one of the most popular and effective data security methods used by organizations.

(c) 2021 Lexeprint Inc. All Rights Reserved.



What Does Encryption Protect?

- Messages
- Email
- Passwords
- Bank statements
- Credit card transactions

(c) 2021 Lexeprint Inc. All Rights Reserved.



Purpose of Data Encryption

- To protect digital confidentiality as it is stored on computer systems and transmitted using the internet or other computer networks.
- Modern encryption algorithms now play a crucial role in the security of IT systems and communications.

(c) 2021 Lexeprint Inc. All Rights Reserved.

How Does Encryption Work?

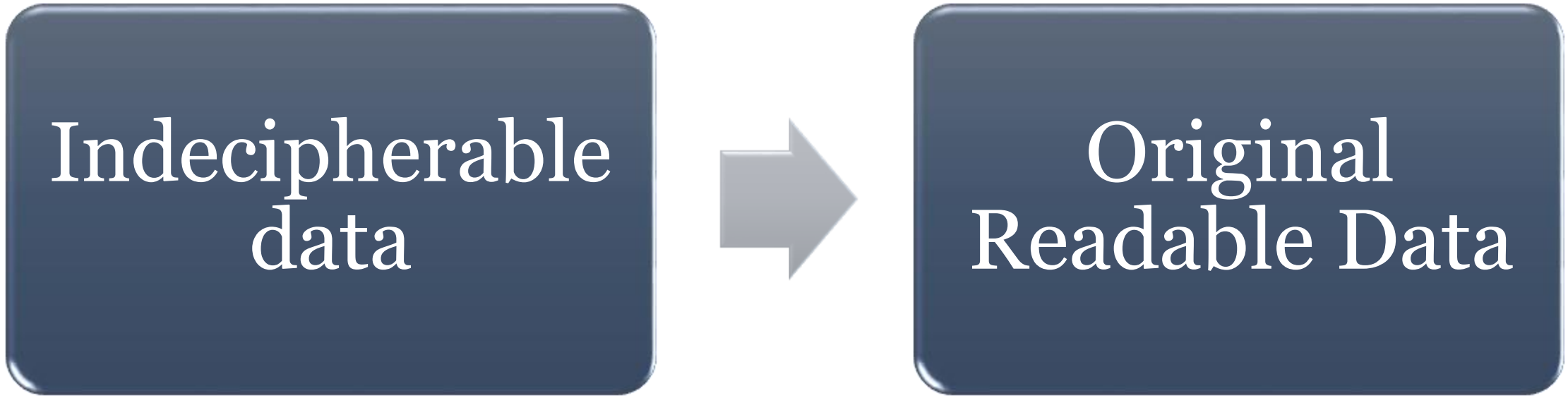
It is not rocket science or is it…



(c) 2021 Lexeprint Inc. All Rights Reserved.

How Does Decryption Work?

Inverse function of encryption



(c) 2021 Lexeprint Inc. All Rights Reserved.

Who Seeks to Access Encrypted Information?

The good and the bad, depending on your personal views



Governmental agencies



Organized criminals



Hackers



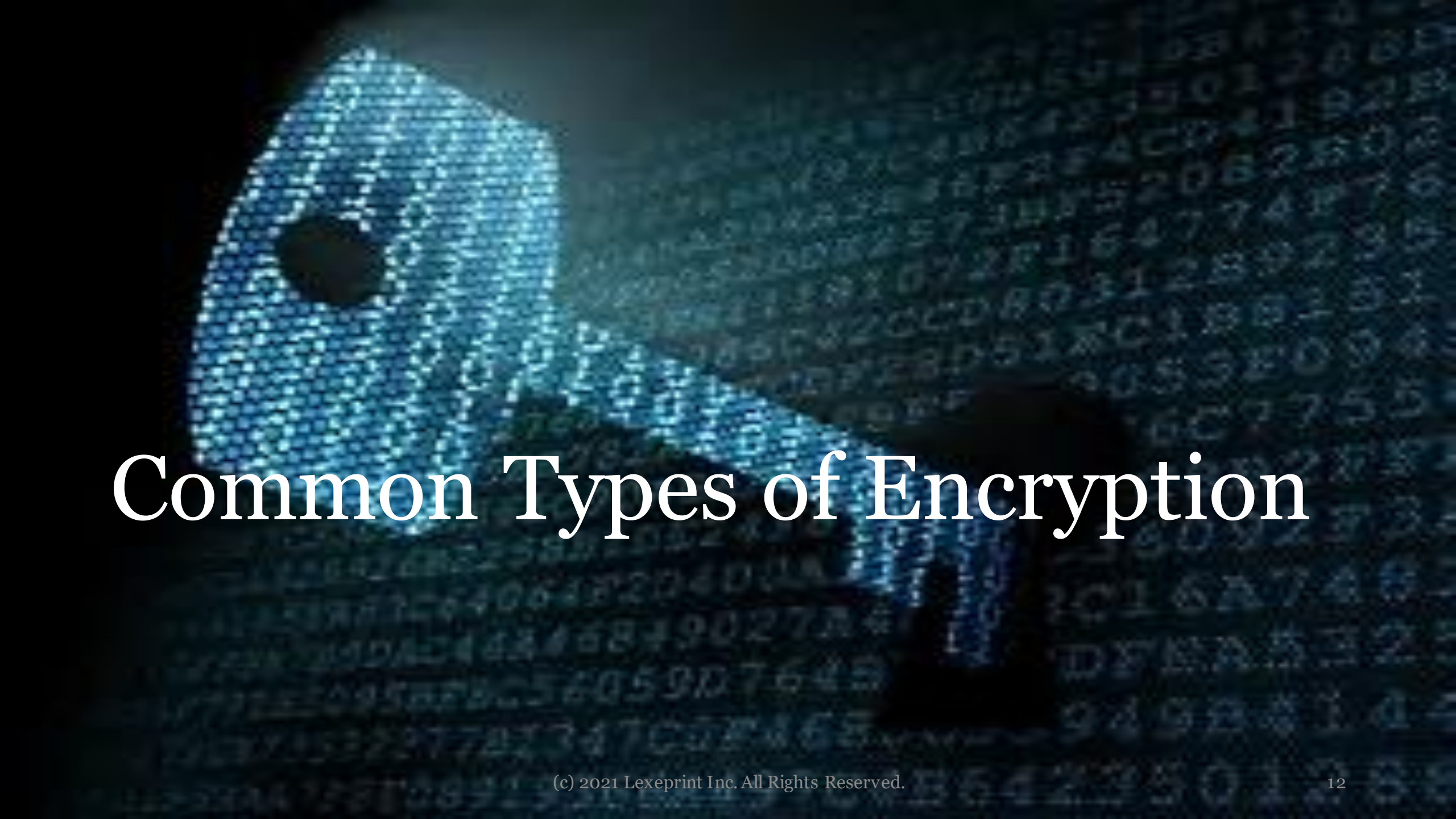
Competitors



Abusive spouses

And the list goes on…

(c) 2021 Lexeprint Inc. All Rights Reserved.



Common Types of Encryption

(c) 2021 Lexeprint Inc. All Rights Reserved.

Types of Encryption

Public Key and Asymmetric Key Encryption

Two keys are created: (1) Public Key and (2) Private Key

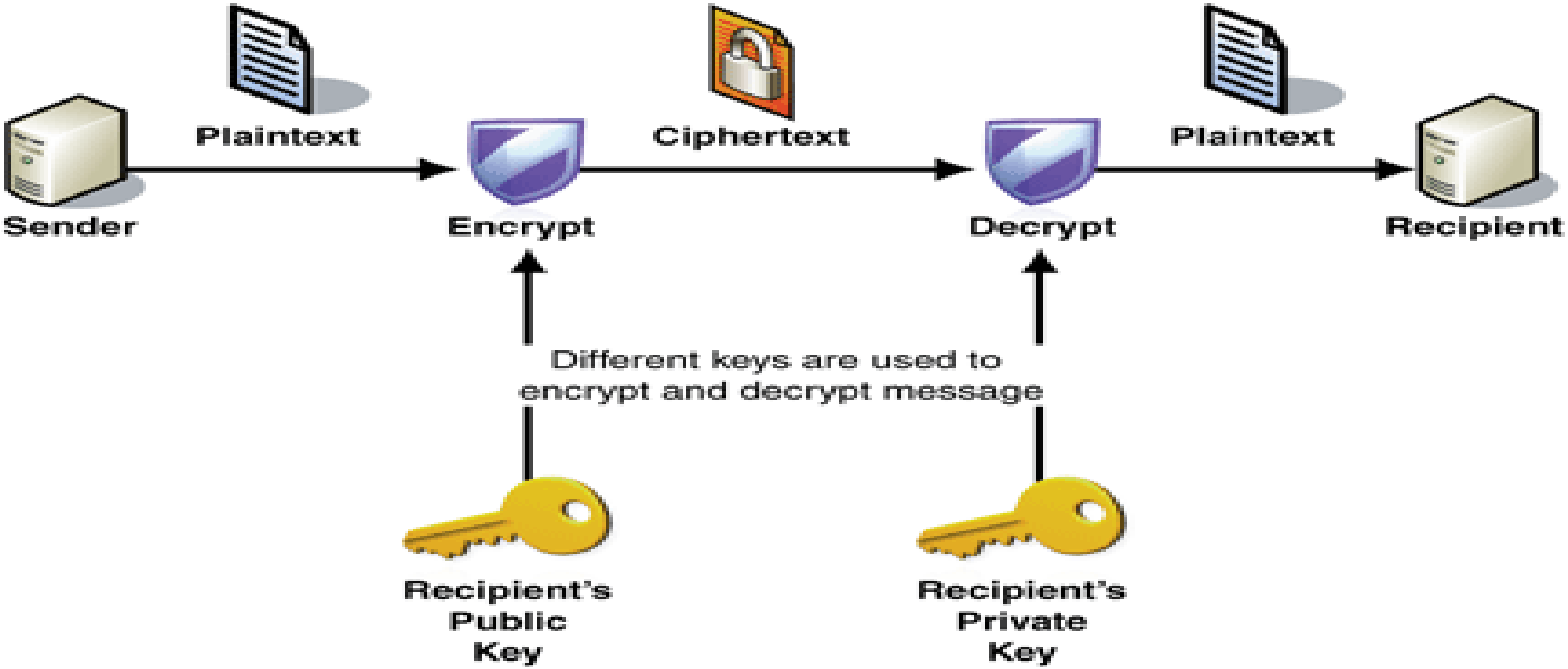
Anyone can encrypt data using the public key created.

Decryption is possible **ONLY** with a private key to access that data

(c) 2021 Lexeprint Inc. All Rights Reserved.

Asymmetric Encryption

Two different mathematically related keys used for encryption and decryption



(c) 2021 Lexeprint Inc. All Rights Reserved.

Symmetric Encryption

Same key used for Encryption and Decryption



(c) 2021 Lexeprint Inc. All Rights Reserved.

Types of Encryption

Private Key and Symmetric Secret Key Encryption



Private Key Encryption

- Data encrypted and decrypted using the same key
- Access is available only to the parties who have the key
- The key must be always kept safe to secure data

(c) 2021 Lexeprint Inc. All Rights Reserved.

Types of Encryption

Hashing or "one-way" encryption



Any piece of data (a password, piece of software, other plaintext data)

- Conversion through a hash algorithm or function.
- Creation of relatively unique fixed length value – "Hash"
- A party can use hash to verify that data has not been altered; however, anyone can change the data and recompute the hash value

(c) 2021 Lexeprint Inc. All Rights Reserved.

Symmetric vs. Asymmetric Encryption

Issues to consider when selecting encryption method.

Asymmetric Encryption

- Used by websites and communication applications where the parties are unable, or do not desire to, share the same cryptographic keys
- Takes time to process data.
- Asymmetric Encryption may consume more computing power than Symmetric Encryption.
- Asymmetric Encryption works with small bits of cleartext.
- Resource costly, that's why used to protect symmetric keys but not data.

Symmetric Encryption

- Both parties require the same key; allows for stronger encryption.
- Usually operates faster than Asymmetric Encryption.
- Does not require a great deal of memory and disk storage
- Works with small bits, medium messages, or large files
- Due to these reasons, used more often to secure data

*Cryptography by Daniel Garrie, Rick Borden and Jeff Stapleton

(c) 2021 Lexeprint Inc. All Rights Reserved.



Key Management Lifecycle

(c) 2021 Lexeprint Inc. All Rights Reserved.

What is Key Management Lifecycle?

This is important to lawyers because…

Key Management

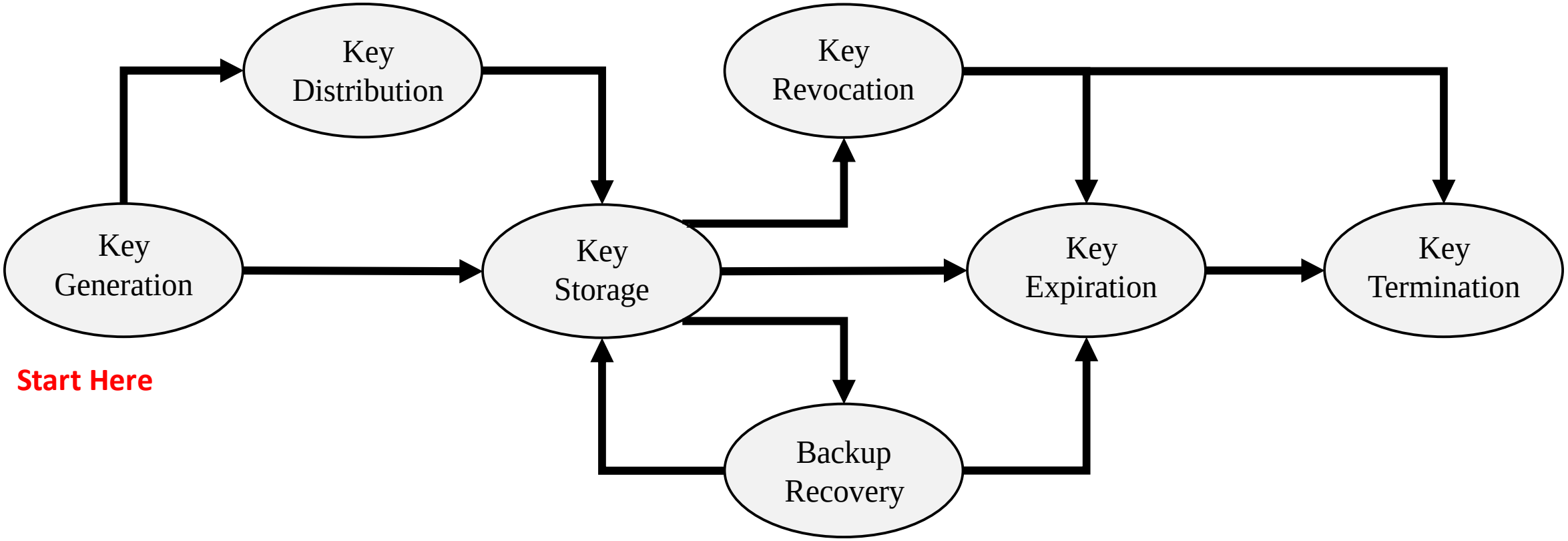


Management of encryption keys in the system that involves seven important stages

(c) 2021 Lexeprint Inc. All Rights Reserved.

Key Management Lifecycle

It all starts with making the key…



(c) 2021 Lexeprint Inc. All Rights Reserved.

Stage 1: Making the Key

You must create something to get the ball rolling.



Symmetric keys are randomly generated, or asymmetric private and public key pairs are mathematically computed

(c) 2021 Lexeprint Inc. All Rights Reserved.

Stage 2: Get the Word Out



Key Distribution:

One or more keys are shared among two or more participants

(c) 2021 Lexeprint Inc. All Rights Reserved.

Stage 3: Key Storage

Need to store the key but they expire



Key Storage:

- Keys are used for their intended purpose (encryption, message authentication, digital signatures etc.).
- Protection of the keys from disclosure, modification, replacement, unauthorized access required.
- Keys have “expiration” date and must be replaced periodically

(c) 2021 Lexeprint Inc. All Rights Reserved.

Stage 4: Key Backup & Recovery

Got to be able to recover the key when necessary

Function can be needed when operational outage is unacceptable due to a disabled key.

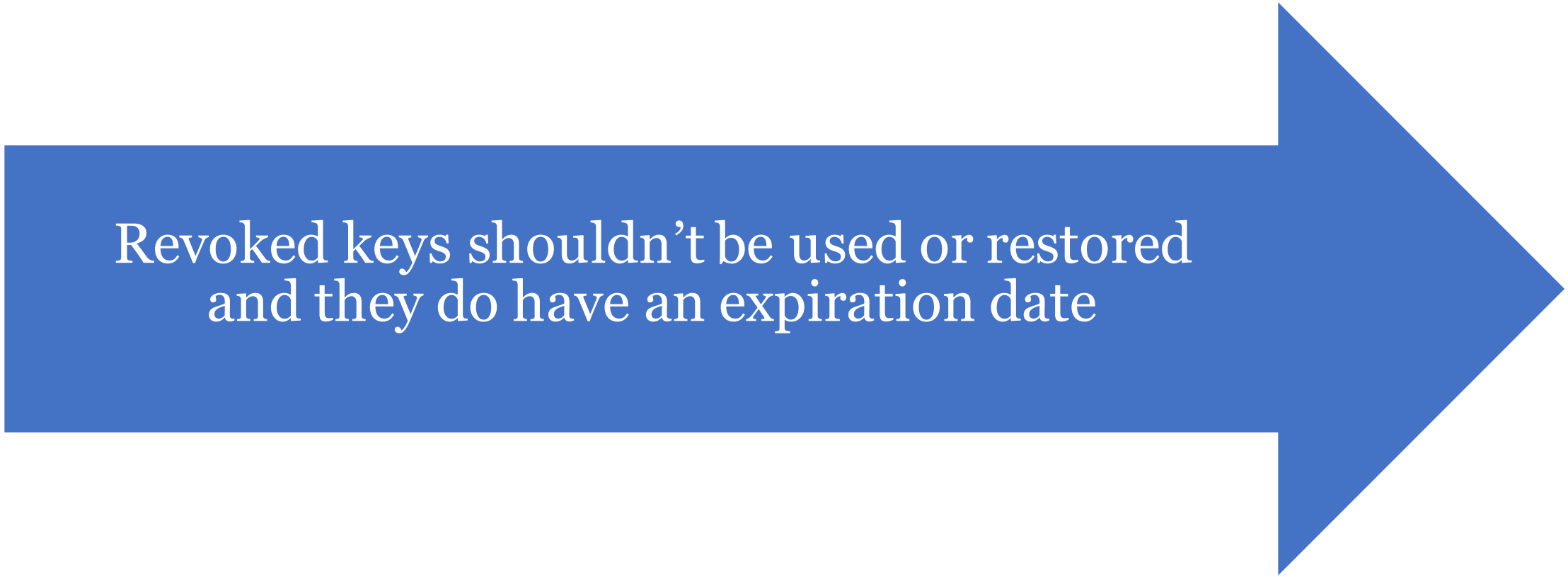
Copies of keys can be stored safely in the event of application failure that might corrupt or erase keys.

Keys can be restored as part of the application process.

(c) 2021 Lexeprint Inc. All Rights Reserved.

Stage 5: Key Revocation

Remember to destroy the keys



(c) 2021 Lexeprint Inc. All Rights Reserved.

Stage 6: Key Expiration

Don't forget.



All keys have an expiration date. Use of the key after that date can result in data compromise or other negative outcomes

(c) 2021 Lexeprint Inc. All Rights Reserved.

Stage 7: Key Termination

You must destroy them to keep the system functioning.

The stage of deleting an expired key.

(c) 2021 Lexeprint Inc. All Rights Reserved.

How to Effectively Control Key Management?

Basic key hygiene goes a long way.



Keys must be kept secure at all times



Replace keys periodically in accordance with their "expiration date"

(c) 2021 Lexeprint Inc. All Rights Reserved.

How to Effectively Control Key Management?

Basic key hygiene goes a long way.



Supervision of the order: who uses it and how



Determination of the terms: how many keys should be used in data back up etc.

(c) 2021 Lexeprint Inc. All Rights Reserved.

New Encryption Rules

(c) 2021 Lexeprint Inc. All Rights Reserved.



DDTC's New FAQ on Encryption Rule's Provision of Access Information and Section 120.50(b)

- On March 25, 2020, the U.S. Department of State's Directorate of Defense Trade Controls (DDTC) interim final rule amended the "Encryption Rule" under the International Traffic in Arms Regulations (ITAR) (22.C.F.R. § 120.54).
- It now addresses more clear definitions explaining activities that are not considered to be exports, reexports, retransfers or temporary imports of secured and unclassified technical data.

(c) 2021 Lexeprint Inc. All Rights Reserved.



DDTC's New FAQ on Encryption Rule's Provision of Access Information

- The DTTC issued a new entry in its FAQ about providing access information to a foreign person under the Encryption Rule.

(c) 2021 Lexeprint Inc. All Rights Reserved.



Recent Trends in Cryptography

(c) 2021 Lexeprint Inc. All Rights Reserved.



Trends in Cryptography in 2020

- Move toward a cashless society
- Growth of Decentralized Finance Adoption
- Onset of Central Bank digital currencies

(c) 2021 Lexeprint Inc. All Rights Reserved.



Move Toward a Cashless Society

- The COVID-19 pandemic has halted, disrupted and stopped several industries. People have been forced to rethink their attitude towards remote jobs and crypto payments.
- Remote jobs and crypto payments have become a highlight of 2020 and it appears that they are here to stay, even after the pandemic ends.
- Why work from an office or even spend on luxurious offices when there may no longer be a need?
- Work may be accomplished efficiently from any spot in the world!

(c) 2021 Lexeprint Inc. All Rights Reserved.



Growth of Decentralized Finance Adoption

- Decentralized Finance ("DeFi") is now one of the most prominent trends in crypto since 2019. This sector has been rapidly growing over the past year. The total value in DeFi is at an astonishing new high - $4 billion!
- An impressive number of companies that operate in the blockchain field have already introduced their DeFi products.
- As DeFi is swiftly growing, it will be essential for organizations to have a "simple, effective, inexpensive on-ramp and off-ramp solution for this segment."

(c) 2021 Lexeprint Inc. All Rights Reserved.



Onset of Central Bank Digital Currencies

- Central bank digital currencies ("CBDCs") have become a recent hot topic and a solution in development in many countries.
- One of the world's most extensive tech breeding ground, China, has begun to engage in creating the local digital asset.
- Since then, governments and central banks all around the globe have begun exploring the area, running trials and even launches of central CBDCs.

(c) 2021 Lexeprint Inc. All Rights Reserved.



Worldwide Encryption Trends in 2020

- 48% of organizations have an encryption strategy applied consistently across their enterprise.
- 21% of organizations reported an increase in encryption use within public cloud services over the last 4 years.
- 60% of employees say their organization plans to use blockchain in the near future.

(c) 2021 Lexeprint Inc. All Rights Reserved.

Questions?

(c) 2021 Lexeprint Inc. All Rights Reserved.

Contact Us



David Cass
Email: davidcassciso@gmail.com
URL: https://www.newyorkfed.org/



Sean Walsh
Email: swalsh@zeklaw.com
Phone: (212) 826-5336
URL: http://www.zeklaw.com

(c) 2021 Lexeprint Inc. All Rights Reserved.



David Cass
Federal Reserve Bank of New York – Vice President, Cyber & IT Risk
Contact:
E: davidcassciso@gmail.com
URL: https://www.newyorkfed.org/

David is the Vice President for Cyber & IT Risk for the Federal Reserve Bank of New York. Prior to this role, David served as the Chief Information Security Officer for IBM. He had global responsibility for all aspects of security practices, processes, and policies across the IBM Cloud SaaS business unit.

Previously David served as the SVP & Chief Information Security Officer for Elsevier. Where he lead an organization of experienced legal, risk and security professionals that provided data protection, privacy, security, and risk management guidance on a global basis for Elsevier.

David has extensive experience in IT security, risk assessment, risk management, business continuity and disaster recovery, developing security policies and procedures. He has played a key role in leading and building corporate risk & governance and information security organizations in the financial sector. As the Senior Director of Information Security Risk and Governance for Freddie Mac, David rebuilt the risk and governance function and developed a team to provide risk assessments, methodologies, tools, services, and training to improve the organization's capabilities and maturity. Prior to that he was Vice President of Risk Management for JPMorgan Chase, and was responsible for providing an accurate assessment of the current risk management state, contributing to the future direction of risk management, continuity and disaster recovery capabilities for the organization.

David has a MSE from the University of Pennsylvania, and a MBA from MIT. He is also a frequent speaker at high profile industry conferences, and serves on the Board of Directors for PixarBio Corporation.



Sean Walsh
Zeichner Ellman & Krause LLP – Special Counsel
Contact:
E: swalsh@zeklaw.com
W: (212) 826-5336
URL: http://www.zeklaw.com

Mr. Walsh retired from the U.S. Department of Justice as Assistant General Counsel in the FBI's National Security Law Branch. He has extensive experience in cyber investigations, U.S. cyber policy, and national security matters. He provided legal advice on forensic and cyber matters to the Intelligence Community for their Counter Intelligence and Counter Terrorism programs as well as to the Foreign Intelligence Surveillance Court. He served as the national security counsel to the FBI Cyber division and participated in interagency working groups shaping national cyber policy. Mr. Walsh served as Assistant General Counsel to the N.Y. City SCA Inspector General's Office and as a Special Assistant District Attorney in the Manhattan District Attorney's Office focusing on corruption and money laundering in the city's construction industry. He initiated and managed a forfeiture program and fourteen monitorships / private inspector generals in efforts to reform the industry. Mr. Walsh had a law practice that focused on white collar and complex civil litigation and technology matters.

Mr. Walsh was a Bureau Chief in the Bronx District Attorney's Office, where he managed forfeiture, homicides, and forensic investigations of computer, video, and audio evidence. He was chief of the first law enforcement video unit that used video to record suspect statements, crime scenes and lineups. He has lectured extensively all over the world on the use of video by law enforcement to enhance their cases. He pioneered the use of a remote video link (VTC) for use in New York courtrooms. He has investigated and prosecuted computer crime cases using forensics and management of digital information. He has lectured extensively on computer security matters including at the European Union computer crime conference at The Hague. Mr. Walsh, as a representative of the United States government, participated in the London training of the Iraqi judges for Iraqi Special Tribunal that conducted the Iraq war crime trials.

Mr. Walsh is also an adjunct faculty member at the New Jersey Institute of Technology College of Computing where he teaches a course on Cyber Investigations, Security, and the Law and assists in their research projects.

Don’t Fall Behind: A Cybersecurity Guide for Law Firms

This concise guide offers steps all law firms, small and large, should take to protect their networks and data against cyber attacks.

Buy Now

By Daniel B. Garrie

Available on Amazon as an eBook or paperback.