

Block This Way: Securing Identities Using Blockchain

Traditional PKI Concepts

James D. Argue, CISSP, MCSE
Team Lead, Network Security Architect
Information Security Branch



OCIO

Office of the Chief Information Officer

19th Annual Privacy and Security Conference
February 7, 2018

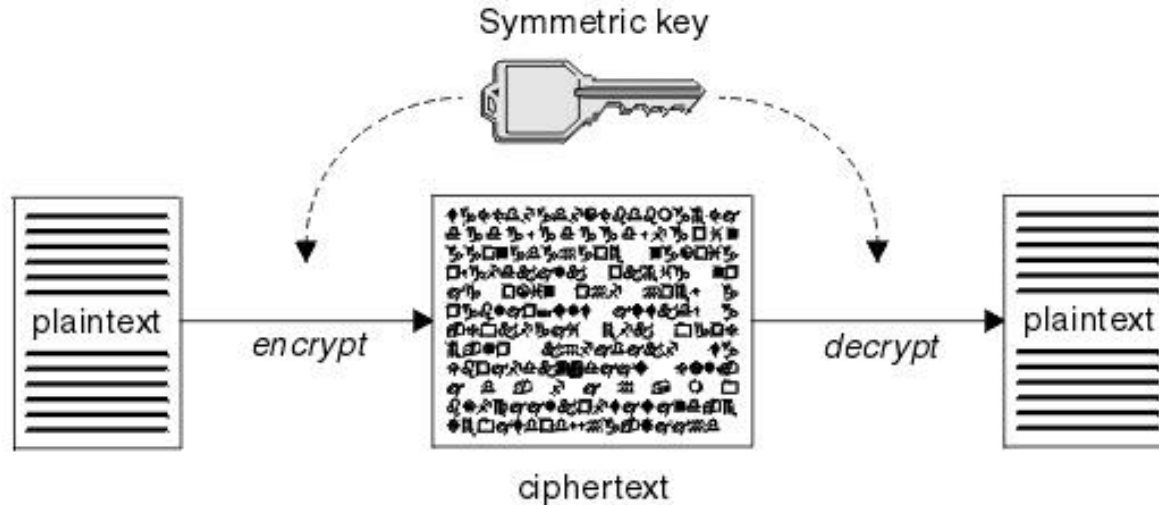
Traditional PKI Concepts

- Symmetric cryptography
- Asymmetric cryptography (public / private keys)
- Certificate Authority
- Certificate Revocation Lists
- Key* Management Systems - Historical - Centralized, Self-Managed

* "Keys" are just big numbers

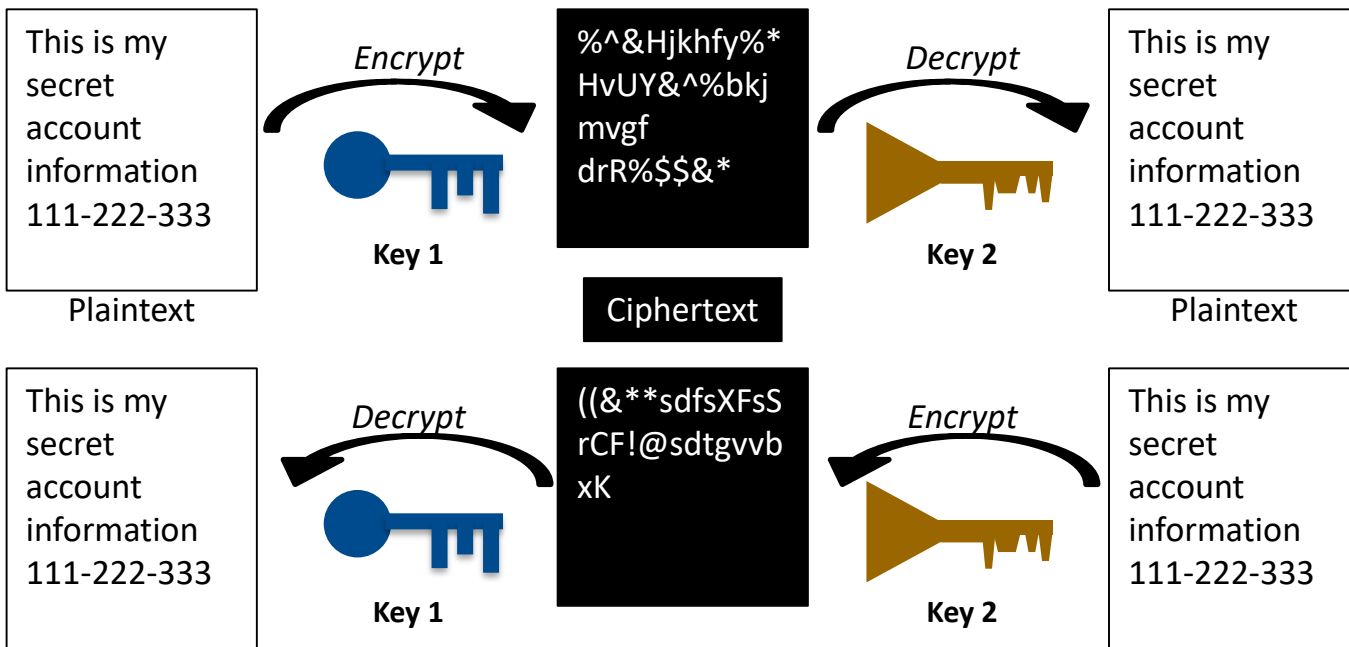
Symmetric Cryptography

- Same key used to encrypt and decrypt, similar to secure zip file with password or a deadbolt lock



Asymmetric Cryptography

- Two complimentary keys; two inverse functions

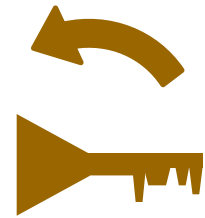
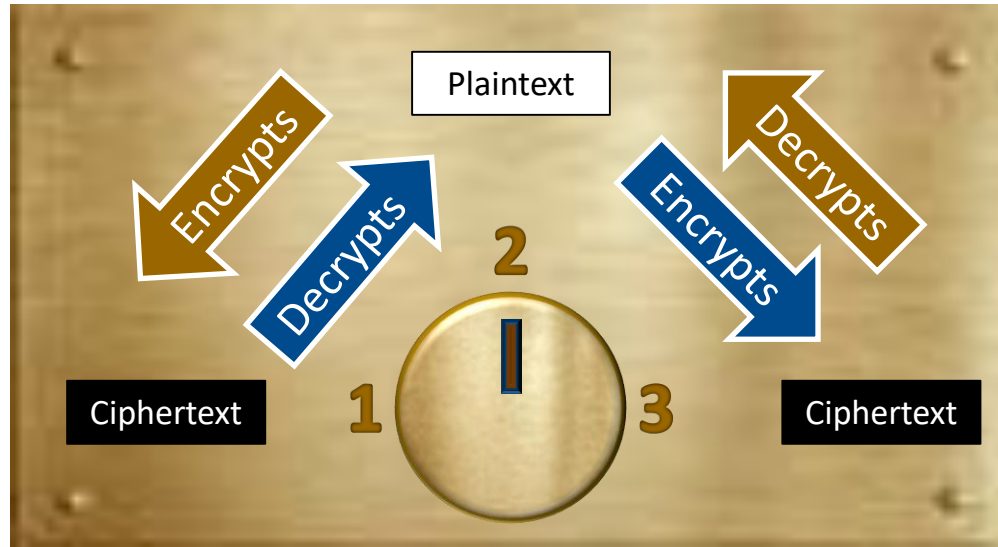


Asymmetric Cryptography Analogy

- Like a special 3 – position lock
- Each key only turns one direction – opposing its paired partner



Key 1
*Suppose
moves
right only*

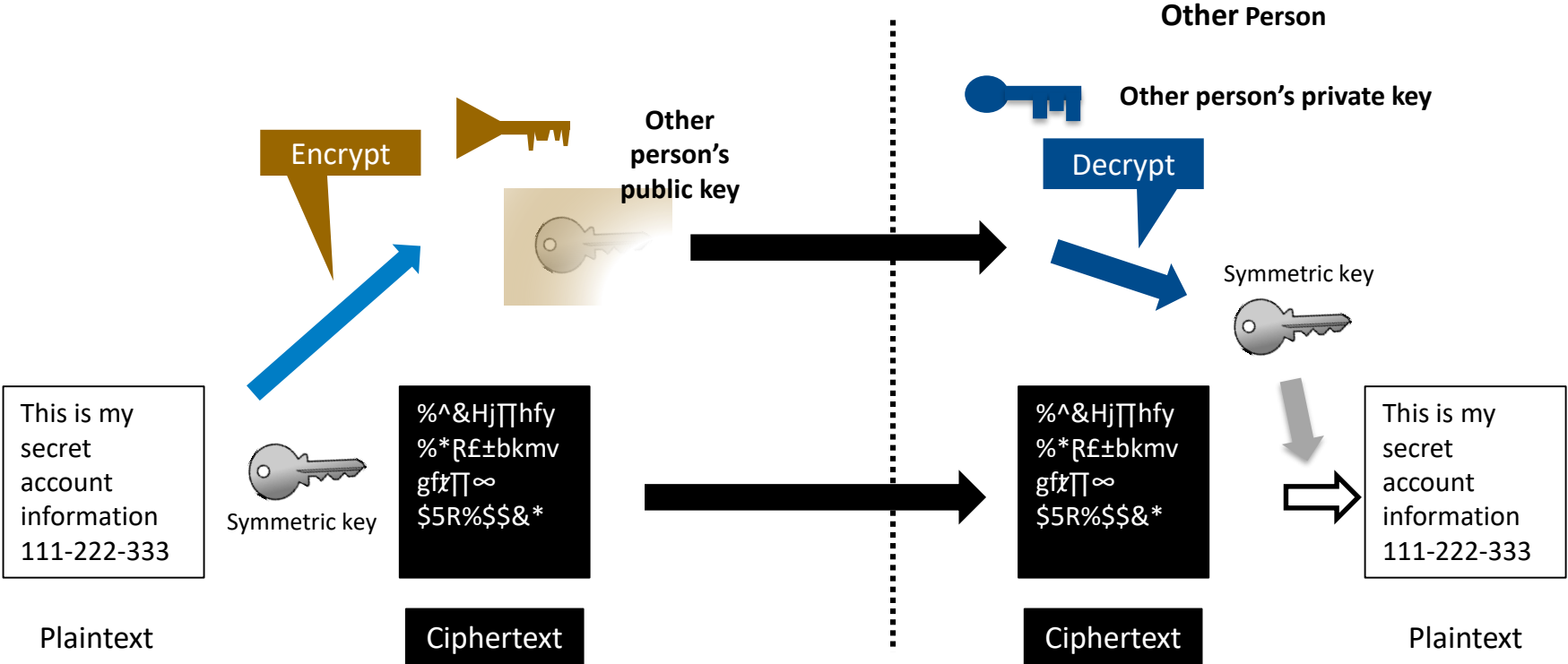


Key 2
*Suppose
moves
left only*

Hybrid Cryptography

- Asymmetric crypto is slow—calculating factors and modulus using large numbers (2048+ bit)
- Symmetric crypto is ~1000x faster—calculates with XOR and multiplication using smaller numbers (256 bit)
- Asymmetric keys are paired and each could be public or private; the private key stays private (*wow, that's deep*)
- Symmetric can encrypt/decrypt and keys shared using asymmetric

PKI - Encryption



Hash – no ‘undo’

1. Cannabis resin
2. (food) A coarse mixture of ingredients
3. (a.k.a. digest/checksum) Encoding of data into a small, fixed-sized chunks to verify message authenticity and integrity.
 - Output length is small compared to input
 - Computation is fast and efficient for any input
 - Any change to input affects lots of output bits
 - Irreversible, one-way value -- input cannot be determined from the output
 - Strong collision resistance -- two different inputs can't create the same output

Margaret Rouse, et al., (2017, November) What is encryption? [whatis.com article]
Retrieved from <http://searchsecurity.techtarget.com/definition/encryption>

Hash Analogy – only one perfect recipe

INGREDIENTS

2 tablespoons olive oil
12 ounces pancetta, sliced in thin strips
1 small red onion
4 tablespoons tomato paste
1 teaspoon red pepper flakes
1 ½ tablespoons chopped parsley
20 ounces canned plum tomatoes, pureed
1 pound bucatini pasta
¼ cup finely grated Parmigiano-Reggiano
¼ cup finely grated Pecorino Romano

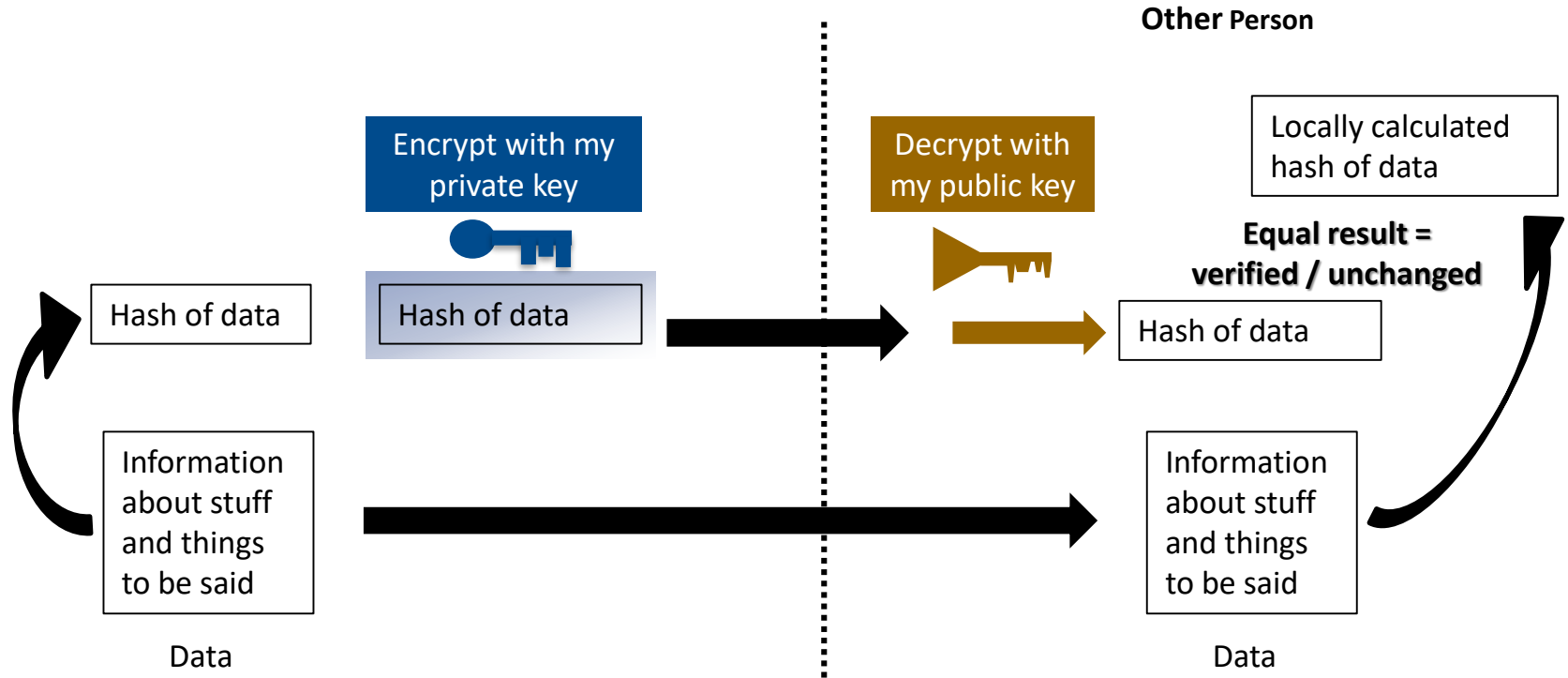


[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

*Those tomatoes won't
ever be the same again!*

- Combining the ingredients again will result in the same great taste!

PKI - Signing

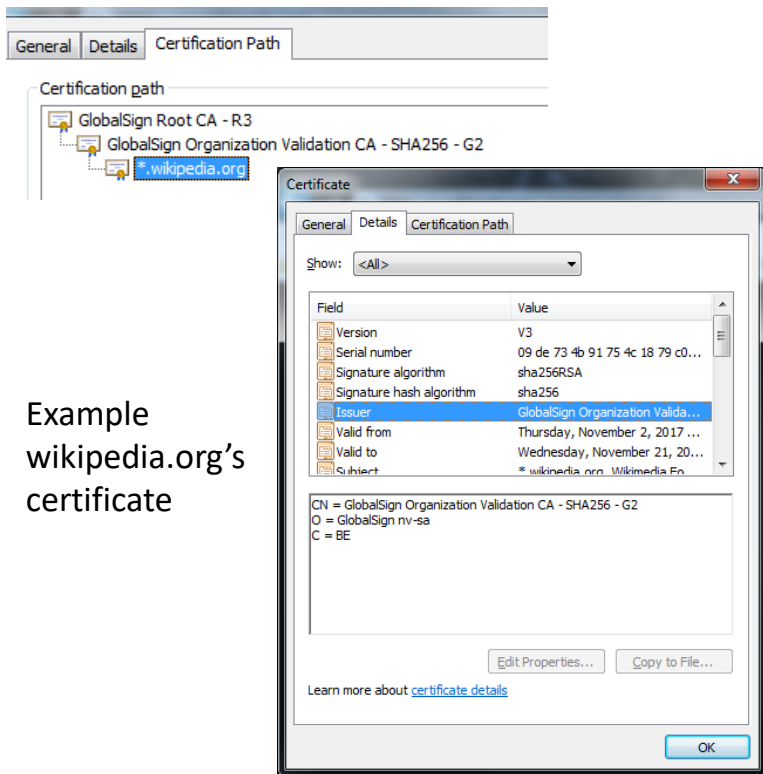


Certificate Authorities

How do we prove we have the public key of the correct individual?

- CA's are trusted through mechanisms and controls
 - Root CA's are self-signed and published, but are built and locked down, such as through a root key ceremony adhering to a certificate policy
- Individual keys are certified by CA's, creating a chain of trust

Chain of Trust



Example
wikipedia.org's
certificate

End-entity Certificate

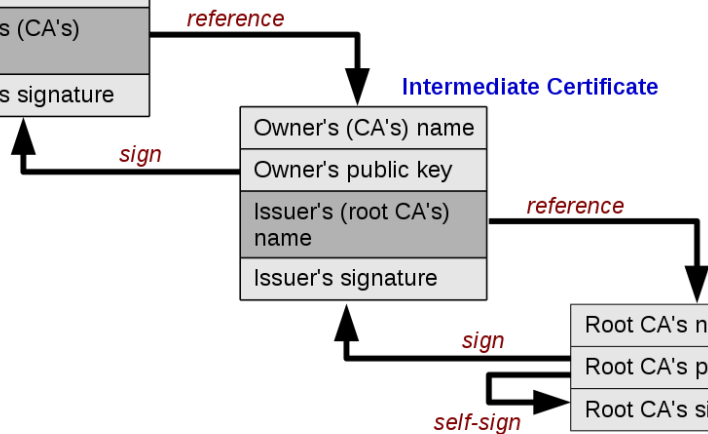
Owner's name
Owner's public key
Issuer's (CA's) name
Issuer's signature

Intermediate Certificate

Owner's (CA's) name
Owner's public key
Issuer's (root CA's) name
Issuer's signature

Root CA's name
Root CA's public key
Root CA's signature

Root Certificate




This Photo by Yanpas is licensed under CC BY-SA

Certificate Revocation List (CRL)

What if a private key is stolen or compromised?

- Certificates come with a validity period that expire a certificate over time
- Administrators can revoke a certificate to show it is invalid before its expiry date
- The Certificate Revocation List Distribution Point (CDP) is a signed, published list of revoked certificates

CDP?



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

Issued to: *.wikipedia.org

Issued by: GlobalSign Organization Validation CA - SHA256 - G2

Valid from 2017- 11- 02 **to** 2018- 11- 21

Validity period

[1]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=<http://crl.globalsign.com/gs/gsorganizationvalsha2g2.crl>

CDP

General Revocation List

Revoked certificates:

Serial number	Revocation date
41 26 d0 42 91 4d 9e 96 06 c8 e8 9b	Tuesday, January 23, 2...
36 07 f7 96 9b 68 4c 8f 25 b5 94 57	Tuesday, January 23, 2...
44 a7 b3 1e 4e bb 3a 9b f1 77 c5 3c	Tuesday, January 23, 2...
03 96 3e 36 4b d1 fe 15 19 73 f7 c8	Wednesday, January 2...

Revocation entry

Field	Value
Serial number	03 96 3e 36 4b d1 fe 15 19 73 f7 c8
Revocation date	Wednesday, January 24, 2018 12:0...

CRL

Centralized Key Management Issues

What if a key or CA is compromised?

- Central storage / lucrative target
- Same keys protect data from multiple applications (user centric)
- Multiple trusted root CA's – duplicate certs possible for same site name signed under different root CA's

Matt Nordoff, (2013, November 17). What happens when a root CA has its private key compromised? [stackexchange.com message board answer]

See <https://crypto.stackexchange.com/questions/11714/what-happens-when-a-root-ca-has-its-private-key-compromised>

References and links

- *(recommended by James)*
Panayotis Vryonis, (2013, August 28). public-key cryptography for non-geeks [blog post]
<https://blog.vrypan.net/2013/08/28/public-key-cryptography-for-non-geeks/>
- Anthony Vance, (2014, October 14). How the RSA algorithm works, including how to select d , e , n , p , q , and ϕ (phi), [YouTube video]
<https://www.youtube.com/watch?v=Z8M2BTscoD4>
- Why can't you decrypt an encrypted message with just the public key? (2014, August 14).
<https://crypto.stackexchange.com/questions/18658/why-cant-you-decrypt-an-encrypted-message-with-just-the-public-key>
- Speed Advantage of Symmetric Key Encryption (2011, July 25).
<https://stackoverflow.com/questions/6812227/speed-advantage-of-symmetric-key-encryption>
- How does a public key verify a signature? (2015, August 15).
<https://stackoverflow.com/questions/18257185/how-does-a-public-key-verify-a-signature>
- *(James' WARNING: Math!!)*
Is it possible to decrypt a ciphertext with a different private key? (2016, December 24).
<https://crypto.stackexchange.com/questions/42524/is-it-possible-to-decrypt-a-ciphertext-with-a-different-private-key>
- RSA encryption with private key and decryption with a public key (2012, March 18).
<https://crypto.stackexchange.com/questions/2123/rsa-encryption-with-private-key-and-decryption-with-a-public-key>
- Digital Signature (2018, February 1).
https://en.wikipedia.org/wiki/Digital_signature
- Electronic Signature (2017, December 7).
https://en.wikipedia.org/wiki/Electronic_signature

References and links (continued)

- Art of the Problem, (2012, February 4). Public Key Cryptography: Diffie-Hellman Key Exchange (short version) [YouTube video] <https://www.youtube.com/watch?v=3QnD2c4Xovk>
- Nick Sullivan, (2013, October 24). (A (Relatively Easy To Understand) Primer on Elliptic Curve Cryptography [Cloudflare article] <https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/>
- *(James' comment: MD5 has been broken since this article, now using SHA-2 family+)*
Steve Friedl, (2005, May 9). An Illustrated Guide to Cryptographic Hashes [Unixwiz.net article] <http://www.unixwiz.net/techtips/iguide-crypto-hashes.html>
- Margaret Rouse, et al., (2017, November). What is encryption? [whatis.com article] <http://searchsecurity.techtarget.com/definition/encryption>
- Matt Nordoff, (2013, November 17). What happens when a root CA has its private key compromised? [stackexchange.com message board answer] <https://crypto.stackexchange.com/questions/11714/what-happens-when-a-root-ca-has-its-private-key-compromised>



James D. Argue

OCIOSecurity@gov.bc.ca