Cryptography with Google Tink

Prof Bill Buchanan OBE, The Cyber Academy

http://asecuritysite.com

CYBER ACADEMY

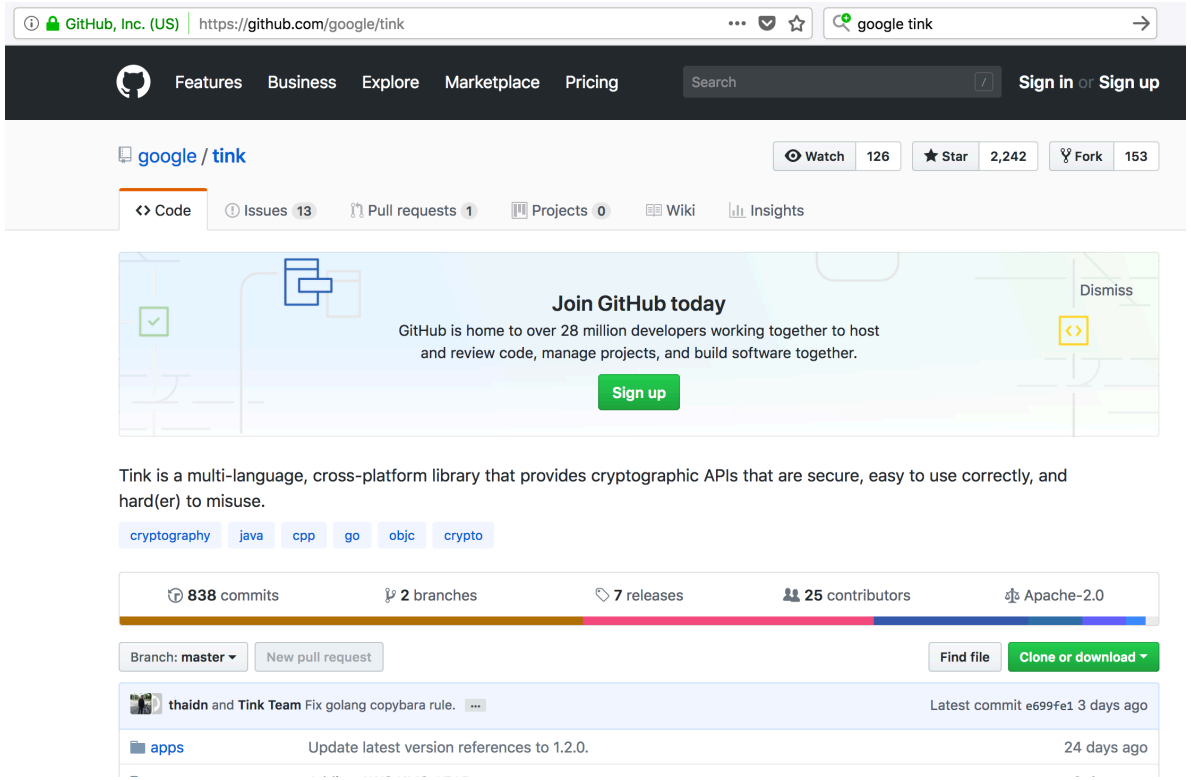
OpenSSL to Tink

OpenSSL
Cryptography and SSL/TLS Toolkit

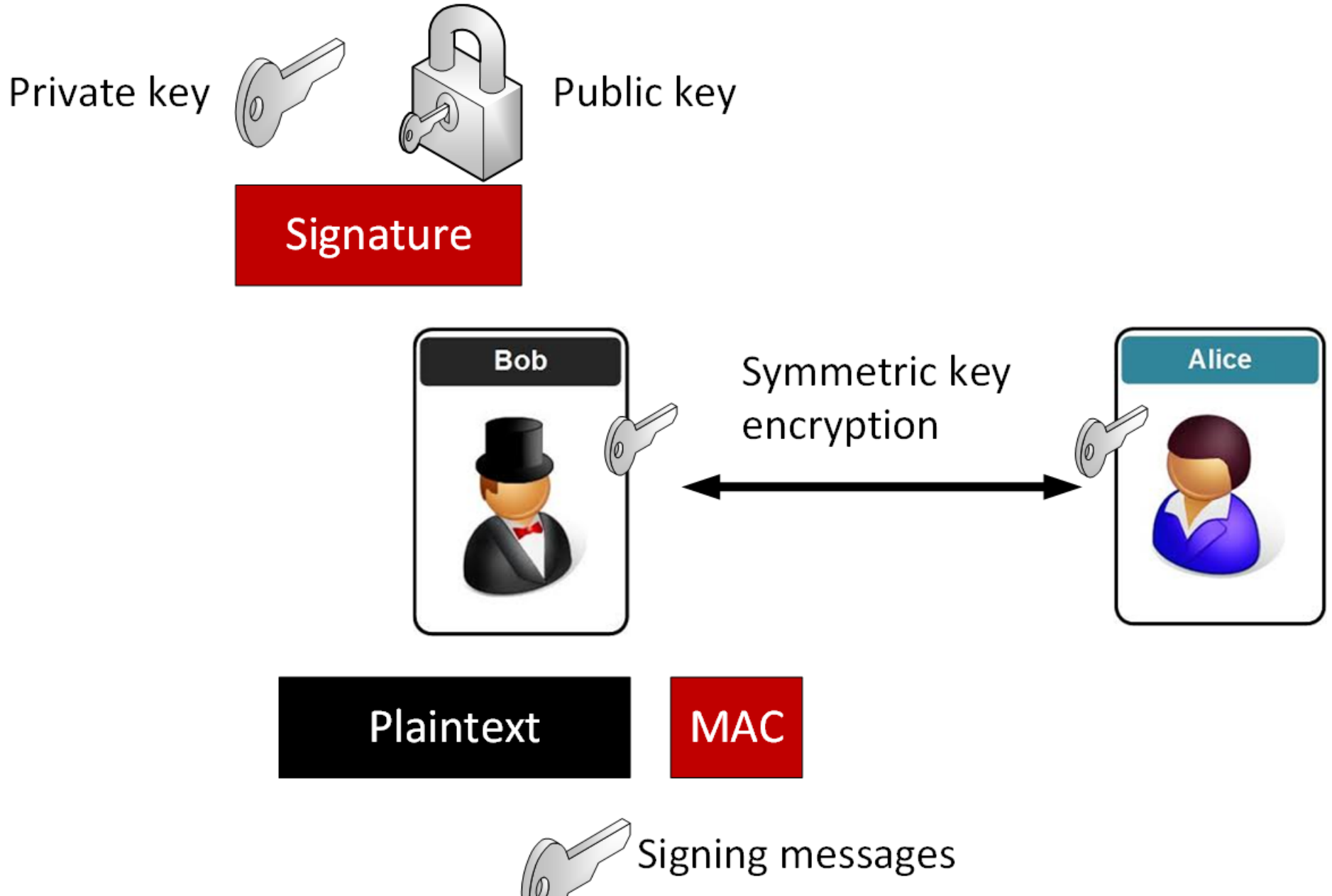
LOGJAM

Forks:

LibreSSL
BoringSSL



Overview


Private key
Public key
Signature
Bob
Alice
Symmetric key encryption
Plaintext
MAC
Signing messages

Cryptography with Google Tink: Symmetric Encryption

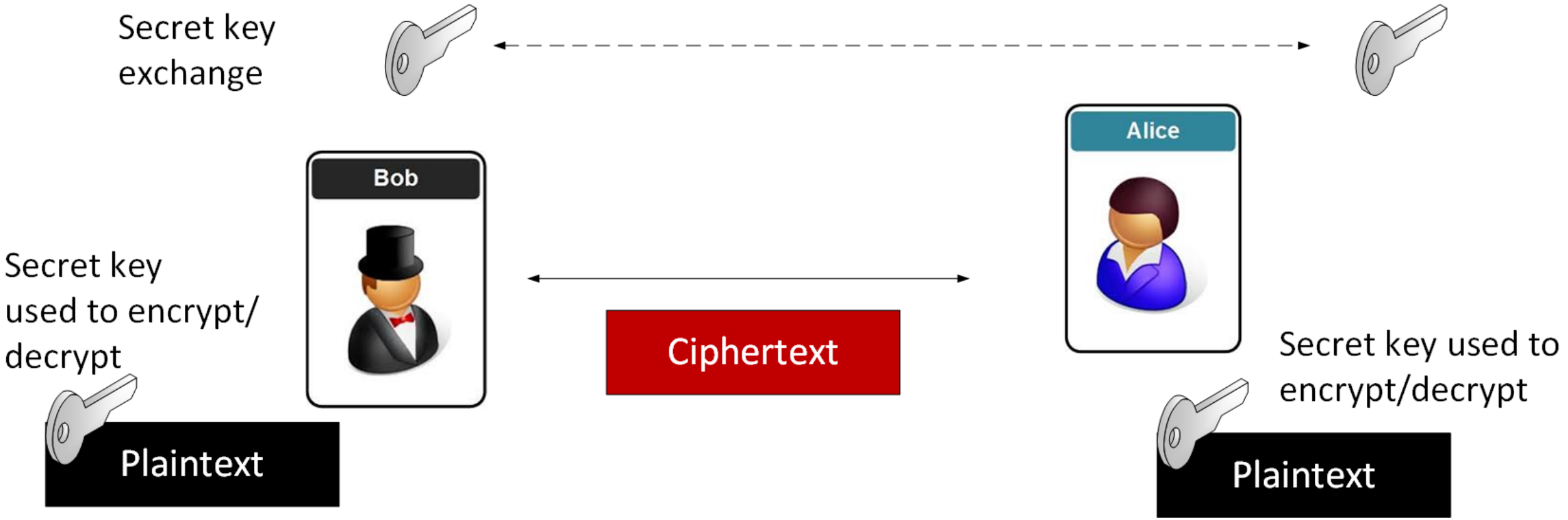
Prof Bill Buchanan OBE, The Cyber Academy

http://asecuritysite.com

CYBER ACADEMY

Symmetric Key with Tink

Link



```
AeadConfig.register();
try {KeysetHandle keysetHandle =
KeysetHandle.generateNew(AeadKeyTemplates.AES128_GCM);
Aead aead = AeadFactory.getPrimitive(keysetHandle);

String plaintext="napier";
String aad="qwerty123";
System.out.println("Text:"+plaintext);
byte[] ciphertext = aead.encrypt(plaintext.getBytes(), aad.getBytes());

System.out.println("Cipher:"+ciphertext.toString());
byte[] decrypted = aead.decrypt(ciphertext, aad.getBytes());
String s = new String(decrypted);
System.out.println("Text:"+s);.getBytes());
```

Link

```
AeadConfig.register();
try {KeysetHandle keysetHandle =
KeysetHar
Aead aead

String plai
String aad
System.ou
byte[] cipl

System.out.println("Cipher:"+ciphertext.toString());
byte[] decrypted = aead.decrypt(ciphertext, aad.getBytes());
String s = new String(decrypted);
System.out.println("Text:"+s);.getBytes());
```

```
Text: hello123
Password: qwerty
Type: 1
Enc type: 128-bit AES GCMCipher: AQbLoE0ino8ofgrvuSSLOKTaYjdPc/
ovwWznuMeYfjP+TO1fc6cn7DE=Cipher:
4151624C6F4530696E6F386F666772767553534C4F4B5461596A6450632F6F
7677577A6E754D6559666A502B544F31666336636E3744453DDecrypted:
hello123
```

Link

```
AeadConfig.register();
try {KeysetHandle keysetHandle =
KeysetHar
Aead aead

Strin
Strin
Syste
byte

Syste
byte
Strin
Syste
```

Text: hello123
Password: qwerty


```
{
    "primaryKeyId": 1525489658,
    "key": [{
        "keyData": {
            "typeUrl": "type.googleapis.com/google.crypto.tink.AesGcmKey",
            "keyMaterialType": "SYMMETRIC",
            "value": "GhAmZA23Todsp2JPRj7u8130"
        },
        "outputPrefixType": "TINK",
        "keyId": 1525489658,
        "status": "ENABLED"
    }]
}
```

Cryptography with Google Tink: Signing a Message

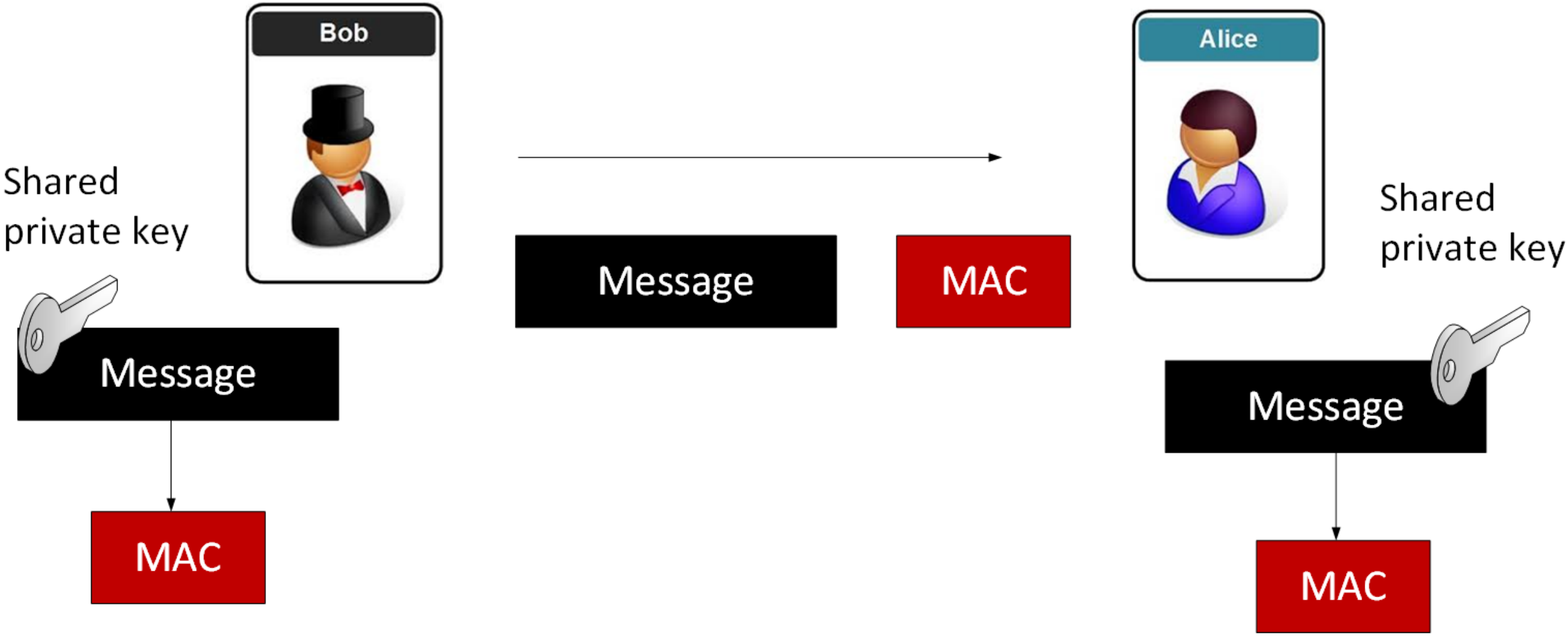
Prof Bill Buchanan OBE, The Cyber Academy

http://asecuritysite.com

CYBER ACADEMY

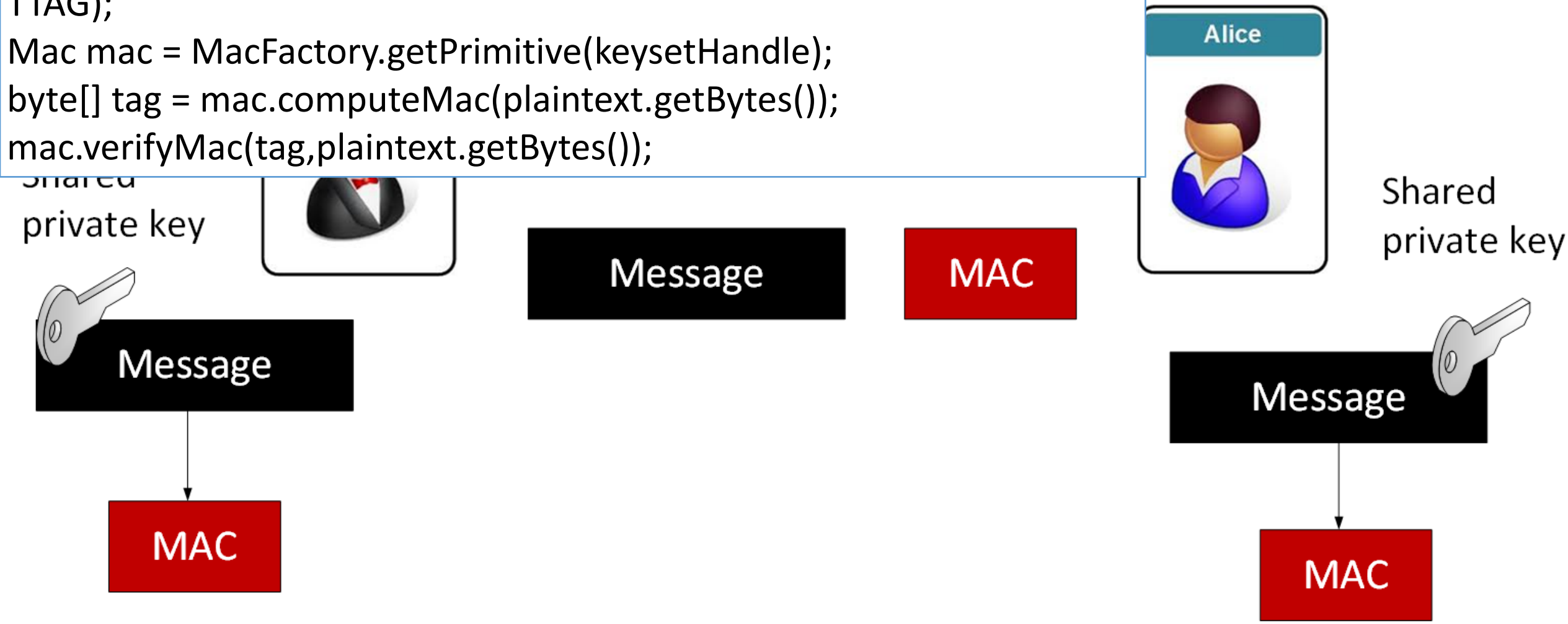
Signing a Message with Tink

Link



```
KeysetHandle keysetHandle =
KeysetHandle.generateNew(MacKeyTemplates.HMAC_SHA256_128BI
TTAG);
Mac mac = MacFactory.getPrimitive(keysetHandle);
byte[] tag = mac.computeMac(plaintext.getBytes());
mac.verifyMac(tag,plaintext.getBytes());
```

[Link]



```
KeysetHandle keysetHandle =
KeysetHandle.generateNew(MacKeyTemplates.HMAC_SHA256_128BI
TTAG);
Mac mac = MacFactory.getPrimitive(keysetHandle);
byte[] tag
mac.verify
```

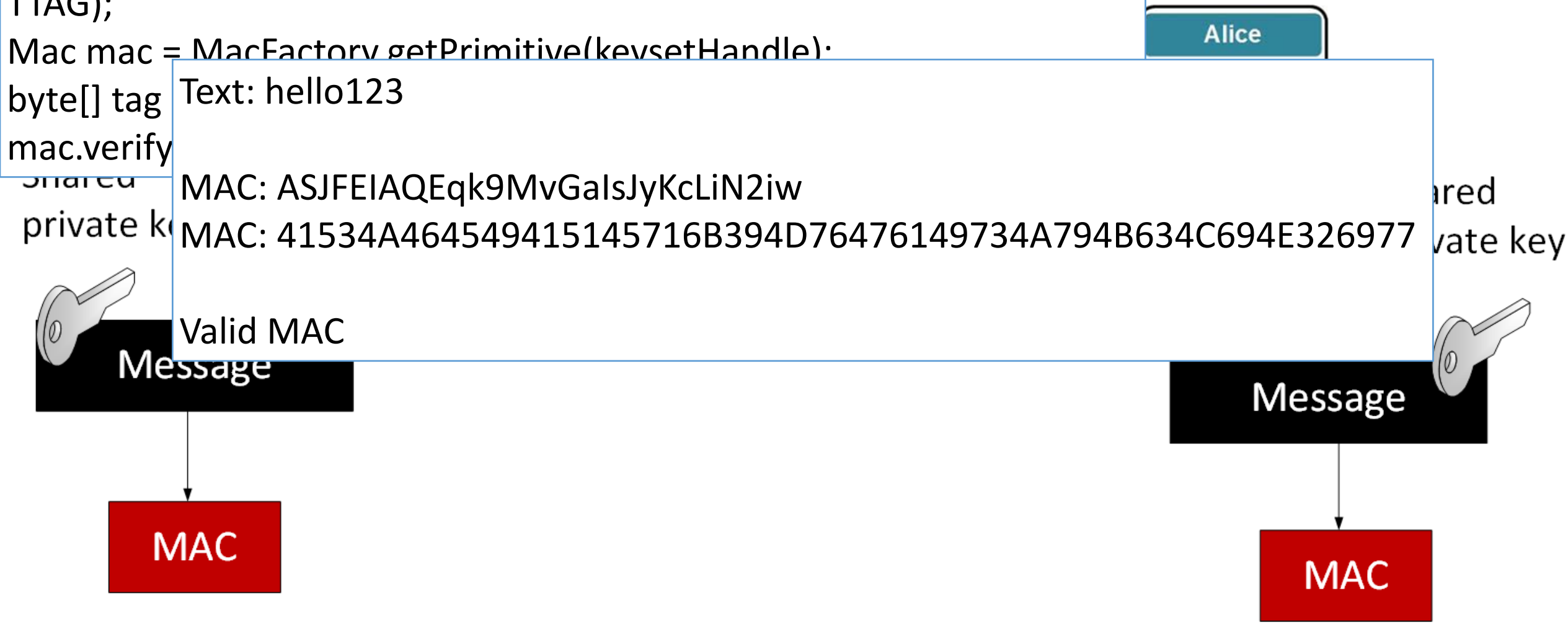
[Link]

Text: hello123

MAC: ASJFEIAQEqk9MvGaIsJyKcLiN2iw

MAC: 41534A4645494151457 16B394D76476149734A794B634C694E326977

Valid MAC



```
KeysetHandle keysetHandle =
KeysetHandle.generateNew(MacKeyTemplates.HMAC_SHA256_128BI
TTAG);
Mac mac = MacFactory.getPrimitive(keysetHandle);
byte[] tag
m
```

Link

Text: hello123

MAC:


```
{
    "primaryKeyId": 574951552,
    "key": [{
        "keyData": {
            "typeUrl": "type.googleapis.com/google.crypto.tink.HmacKey",
            "keyMaterialType": "SYMMETRIC",
            "value": "EgQIAxAQGiAU/p0/1SEV+O1WE/fvQufi7z+rxQ0W6cJeRtgHHtqMQg=="
        },
        "outputPrefixType": "TINK",
        "keyId": 574951552,
        "status": "ENABLED"
    }]
}
```

Cryptography with Google Tink: Digital Signing

Prof Bill Buchanan OBE, The Cyber Academy

http://asecuritysite.com

CYBER ACADEMY

Signing With Tink

Link

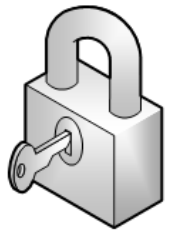

```
{
    "primaryKeyId": 835639698,
    "key": [{
        "keyData": {
            "typeUrl": "type.googleapis.com/google.crypto.tink.EcdsaPrivateKey",
            "keyMaterialType": "ASYMMETRIC_PRIVATE",
            "value": "EkwSBggDEAIYAhogafr30IV05SpchJZvJfQ6ChyWxhNIVSjpmztkJ+wYRusiIHCl4fYPSpuISdC18N9OhWQ9jZvky6B
0ytnL97HqafbrGiEAxJzrrM7H3ONlzTRMdoPwWJ/PwkaQ2rCsUK5i3wGZMZQ="
        },
        "outputPrefixType": "TINK",
        "keyId": 835639698,
        "status": "ENABLED"
    }]
}
```

```
KeysetHandle privateKeysetHandle =
KeysetHandle.generateNew(SignatureKeyTemplates.ECDSA_P256);

PublicKeySign signer =
PublicKeySignFactory.getPrimitive(privateKeysetHandle);
byte[] signature = signer.sign(plaintext.getBytes());
```

Link

Bob's Public key



Alice checks the

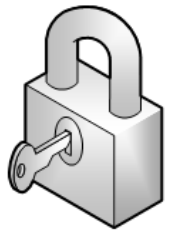

```
{
    "primaryKeyId": 835639698,
    "key": [{
        "keyData": {
            "typeUrl": "type.googleapis.com/google.crypto.tink.EcdsaPrivateKey",
            "keyMaterialType": "ASYMMETRIC_PRIVATE",
            "value": "EkwSBggDEAIYAhogafr30IV05SpchJZvJfQ6ChyWxhNIVSjpmztkJ+wYRusiIHCl4fYPSpuISdC18N9OhWQ9jZvky6B
0ytnL97HqafbrGiEAxJzrrM7H3ONlzTRMdoPwWJ/PwkaQ2rCsUK5i3wGZMZQ="
        },
        "outputPrefixType": "TINK",
        "keyId": 835639698,
        "status": "ENABLED"
    }]
}
```

```
KeysetHandle privateKeysetHandle =
KeysetHandle.generateNew(SignatureKeyTemplates.ECDSA_P256);

PublicKeySign signer =
PublicKeySignFactory.getPrimitive(privateKeysetHandle);
byte[] signature
```

Link

Bob's Public key



hecks the

Text: hello
Sig (Base64):
ATHO2ZIwRAIgd+JV6SOM08i01AFsrGR8JLenLDWtPKzoWUDRh4tBqC8


```
{
    "primaryKeyId": 835639698,
    "key": [{
        "keyData": {
            "typeUrl": "type.googleapis.com/google.crypto.tink.EcdsaPrivateKey",
            "keyMaterialType": "ASYMMETRIC_PRIVATE",
            "value": "EkwSBggDEAIYAhogafr30IV05SpchJZvJfQ6ChyWxhNIVSjpmztkJ+wYRusiIHCl4fYPSpuISdC18N9OhWQ9jZvky6B
0ytnL97HqafbrGiEAxJzrrM7H3ONlzTRMdoPwWJ/PwkaQ2rCsUK5i3wGZMZQ="
        },
        "outputPrefixType": "TINK",
        "keyId": 835639698,
        "status": "ENABLED"
    }]
}
```

Cryptography with Google Tink

Prof Bill Buchanan OBE, The Cyber Academy

http://asecuritysite.com

CYBER ACADEMY