



# Kurer for Outlook

Joshua Yuen



# Kurer for Outlook

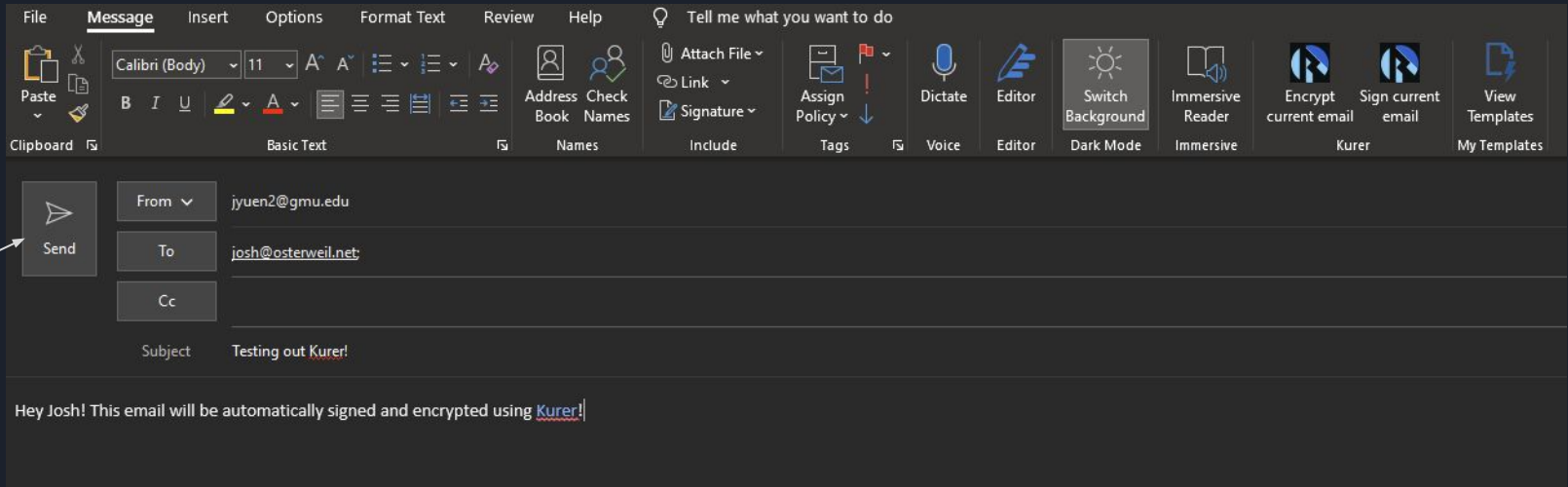
- DANE-based S/MIME encryption and signing
  - No need to exchange public certs beforehand
- Works for any account connected to Microsoft 365 or a Microsoft Exchange server
  - General POP3 or IMAP account support coming soon
- Platform-independent
  - Works in all modern browsers (Chrome, Firefox, Safari, Edge, etc.)
  - Works for Windows client
  - Works for Mac client
- Easily installable with Outlook's usual add-on menu



What can it do?

# Sending Email with Kurer

DONE!



The screenshot displays the Microsoft Word ribbon interface for an email. The 'Message' tab is active, showing various options like 'File', 'Insert', 'Options', 'Format Text', 'Review', and 'Help'. The 'Send' button is highlighted with a white arrow. The email content area shows the following details:

From: jyuen2@gmu.edu  
To: josh@ostenweil.net  
Cc:   
Subject: Testing out Kurer!

The email body text reads: "Hey Josh! This email will be automatically signed and encrypted using [Kurer!](#)"

# Receiving Email with Kurer

By Date ▾ ↑

10:39 AM

Testing out Kurer!


JA Joshua A Yuen <jyuen2@gmu.edu>  
To josh@osterweil.net

Translate message to: English Never translate from: French Translation preferences

Tue 2/1/2022 10:39 AM

Content-Type: application/pkcs7-mime; name=Dsmime.p7m; smime-type=developed-data; charset=binary; attachment; filename=Dsmime.p7m; Content-Transfer-Encoding: base64

S/MIME message detected + Get more add-ins



This email was encrypted to you | This email was signed

Plaintext:

Hey Josh! This email will be automatically signed and encrypted using [Kurer!](#)

REPLY REPLY ALL FORWARD (UNDER DEVELOPMENT)

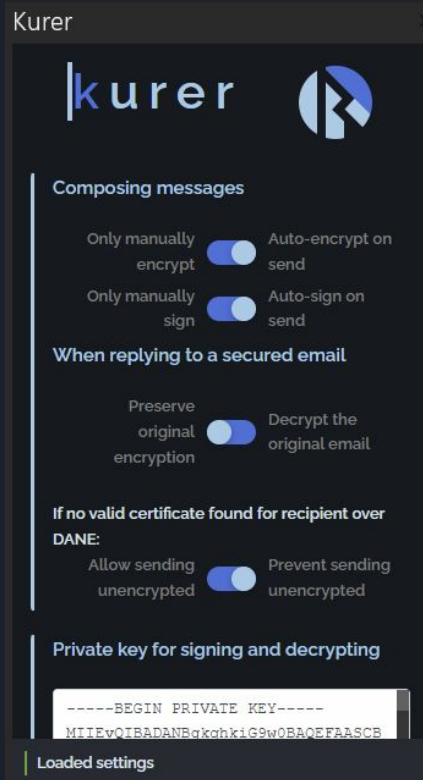
Dsmime.p7m; Content-Transfer-Encoding: base64

BgNVBAYTAiVUwxDjAMBgNVBAMM%0D%  
DVQQKDANNU0wxDjAMBgNVBAMM%0D%  
EAgEFAKEcMBoGCSqGSIb3Q0DQADQEBBCANBgIghkgBZQMEAgEFAASCAQBRTU89t%  
%2BkMjsoy970%2FQB1zHmCzvp5xLmjSWL4%2B%2BupL2E6zqKjv43bzNIEQqE%  
Bsm6K37TvnAS8oPBrTe8dJd6ILMAO3%2Fujzl%0D%  
wMA%2FRMjxQB%2FHYOEdX%0D%0AXYBnitXwLs4%2BfnOckXvfd5qJhR%  
%2B3DQEHATAAdBgIghkgBZQMEAgEFAAEE1i%2B%  
qxwDL%2F2nImI0xsGBRlFdtr1IZSgJWcOyo8GR4OfrrMrt1ddbrajriTY2cfjIT%2FN5Su%  
EsP2dxJ1W8DpMRgdEUlqHw%0D%0APfErW8iz%  
%2B1EeiAyM%0D%0AqH2GviFZ8u7u%  
%2BjLYH%0D%0AU%2Bu2z5YILV2cjYQchhsWgQQTaArZjCKmLs%  
%2BhyyMftT8wh2rYDj6rteWia62yglFRq%2FFJftPWUICuorVcAmfWnGfU13m8Hl61%0D%  
%2B%2Bq5AvzWjGHVNV1jJlfozIN%0D%0AxcOrcPM3mvq8rFYpmTMM2vud%2Ftw%2F8Yv%  
%2BmnjLWTwlQnVcuk1MzvQ4A8tWxy1pgKy9qETIVm4mNtmyaTost28%  
%2B%2B2m%2BwKjAovQx3q8TesJa%2BLuLsJSDdOhc2zszfVnzOdcXZ%0D%0AC%  
%2BpPhDRscBWjEE31nS%0D%0AQpH3Dt%2BYk2XWkUfC4yn5S%2Fyk%2BRRV%  
%2B%2BOKs49raaXumnZzVpyFBfTh%



How?

# Settings



- Options to automatically encrypt and/or sign before sending any email
  - Signs then encrypts with both selected
- Allow your recipient to read text originally encrypted to you
- Fail-safe option for when the recipient doesn't have a DANE cert to encrypt with
  - Set Kurer to prevent unencrypted email from sending
  - Never send an unencrypted email without being *sure*



The recipient had no DANE S/MIMEA public certificate to encrypt with. Allow sending anyways in settings | [Open settings](#) | [Dismiss](#)



The add-in Kurer has prevented this item from being sent. | [Dismiss](#)

# Settings (cont.)

Send Attach Encrypt Discard ...

To Bcc

Cc

Add a subject

Kurer

sign send

If no valid certificate found for recipient over DANE:

Allow sending unencrypted Prevent sending unencrypted

Private key for signing and decrypting

```
-----BEGIN PRIVATE KEY-----
MIIEQwIBADANBgkqhkiG9w0BAQEF
ASCCS0wggkqAgEAAoICAQC2qqtFPQ
/w71/X
h1HY2WE7xVZFBvHGLaT15e2XVFSNF
8faqGopwzRIW1nc7XKOVYDVBJUe5
n1a6Bh
```

[Password to encrypt your private key PEM with (recommended)]

SAVE

Public certificate for signing

```
-----BEGIN CERTIFICATE-----
MIIFPjCCAGeCAQEDQYJKoZIhvcNA
QELBQAwYjELMAkGA1UEBhMCVnXkET
APBqNVBhGmCFZpcmdpbm1hMRAwDgY
DVQOHDAdgWlyZmE4MwQwvCgYDVQOK
DANHTVUxDDAKBgNVBAeMA01TIDESM
B6GL1TTEAooITs8sACB74WUwMB4YDQ
```

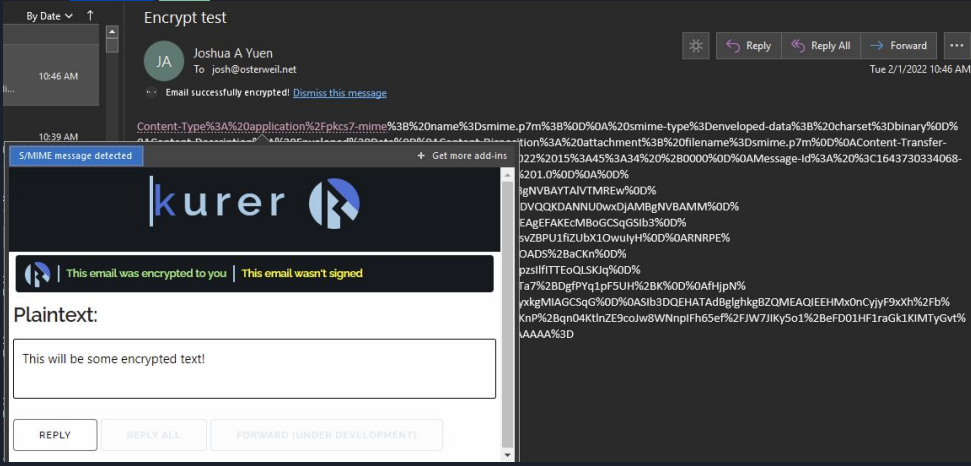
SAVE

sign test! (No subject) Loaded settings

- Configurable private key for signing and decrypting
- Configurable public certificate for signing
  - Input this manually or automatically use your certificate from DANE
- Linked to your Outlook account, synced across all devices
  - Set up once, never worry about it again



# Receiving Encrypted/Signed Emails



- Automatically detect if incoming emails are encrypted or signed
- Simply click the text to automatically decrypt the email and view the plaintext
  - New reply buttons with additional functionality



# Implementation Details

- Settings all stored as key-value pairs in Outlook's cloud--optional password to encrypt private key with
- Standard to send cert alongside signature to verify with--we disregard these and instead use DANE certs for verification
  - Plans in the future to support partial DANE certificates (fingerprints) which this cert will be useful for

# Replying to Encrypted/Signed Emails

- Plaintext will be conveniently viewable at the top of the reply window
  - Will automatically be removed again before sending
- Same automatic signing/encrypting applies

By Date ▾ ↑ RE: Encrypt test

10:48 AM

JA Joshua A Yuen  
To: Joshua A Yuen

Tue 2/1/2022 10:48 AM

Content-Type: multipart/application; format=rtfm; name="3Dsmime.p7m"; charset="utf-8"; boundary="3Dsmime.p7m"; smime-type="developed"; data-bin="3Dsmime.p7m"; data-description="3Dsmime.p7m"; data-disposition="attachment"; filename="3Dsmime.p7m"; content-transfer-encoding="base64"; date="Tue, 2 Feb 2022 02:01:53AAT73A30%20%20B000%0D%0AMessage-Id%3A%20%3C1643730450819-01.0%0D%0A%0D%0D%BgNVBA...";

S/MIME message detected + Get more add-ins

**Plaintext:**

This email was encrypted to you | This email wasn't signed

I'm replying to this encrypted email with an encrypted email of my own!

**From:** Joshua A Yuen  
**Sent:** Tuesday, February 1, 2022 10:46 AM  
**To:** josh@osterweil.net  
**Subject:** Encrypt test

BgNVBA...  
DVQQK...  
EAgEFA...  
fE3Kwx...  
5bsyIP...  
uWAK6...  
0ASib3...  
Kae7LP...  
/f%2FL...  
F7hmTE...  
2Fxs%2...  
jOZztR...  
iD3R1T...  
DqfUCk...  
jBRTqeo...  
jHh7%0...  
5StVN%...  
sqggEx...  
fTddhZ...



Kurer will available for public  
installation soon