#### Joey Navarrete

CYSE 409: Crime and Computer Applications

11/9/2022

## Asymmetric (Public-Key) Symmetry

# Part 1: Answering Questions about encryption

- 1. A separate public and private key are required for online communications between people because if not, the messages can be easily decrypted.
- 2. The main difference between symmetric and asymmetric cryptography is what keys are used. In symmetric cryptography, one single key is used to both encrypt and decrypt communications. In asymmetric cryptography, two separate keys, public and private, are used to encrypt and decrypt communications respectively.
- 3. A person's public key can be shared by placing it in a public space, for example a social media account or a website.
- 4. Signing a message means that the message was initially written by a person and was not changed.
- 5. The algorithm that is used most to encrypt messages is the RSA (Rivest-Shamir-Adleman) algorithm.

## Part 2: Practice with Keys

11/9/2022

6.

-----BEGIN PGP PUBLIC KEY BLOCK-----Version: Keybase OpenPGP v1.0.0 Comment: https://keybase.io/crypto

xo0EY2xCcgEEAMMkxiM/ySW6LyINqfJUBFF2MUrZp1KSA5bUnihHoxhvesa8DCdQ RvTLSfdv00mvafydLjeGgsorrGgvKHYwxYWaovTbetQQLz+tCIxkrxdEJpsGxQb0 5101pmiRnx4PtQ1TRaJ22AJu16DeU1cX1yzpxEjVybE3S6uGoDpu7ck1ABEBAAHN H0Jlbm55IFNtaXRoIDxub3RyZWFsQGVtYWlsLmNvbT7CrQQTAQoAFwUCY2xCcgIb LwMLCQcDFQoIAh4BAheAAAoJEJR34dBvfze05f8EALXuI8uIqxxSZANpgZ93Zxqf OVYXMuq91AqWPYNoYuxSYJ3NGdaO8ntdwpx59z2LWg4qgjbvPkayehlTsKdN/m13 C/SUlCslIiQZ38UwCUIpQIKg+e+ZebkWQ4TSDM800bdw2n9GQWWDmbKRvdk1htTx G73p2Pi5eC2QezLgPKA2zo0EY2xCcgEEALQgE+YUBI3RwCPz0eHFAZ+vF0Jsk/v9 rYT98gU7eWQNYTvwDRQ+Imwn1pX7k08xHh/5r5bXN0fJJPpnGq7IKYeXa1yMR2F3 nVicQ9HDM44wZm8+nbKbnWmwKNl4gulNyqBWYTm9j0wdNcwxLtok47rU/LuDEtdH +L5zNZVqREpPABEBAAHCwIMEGAEKAA8FAmNsQnIFCQ8JnAACGy4AqAkQlHfh0G9/ N7SdIAQZAQoABgUCY2xCcgAKCRAT98T66itt1XTzA/92xIiXg0Jut0sQ0LBLjSvt p6TZgsnDbfd0ZkiaLTaB3E+j7qFw/KQHf3mEiT6LE53gyCv4GI0yU/6P7GgwEzJ8 YpBOD8Uzak4UdWBVwxOvIOR6eN+O3eMsU5AgQZzOKJJDxxOo7Hg3/Ga1ILmIjoWb baCmTS1qzgD08FKUgQSKpVtHBACeTKsAJ5nX0bLmPsCMYvX+VGNwae3zeP9jk3TM KxzOwHdRcwnnfV6YIHC4Ct+fFqp7Yq1mIPByTBjP29REUVJSIvCaEUei1700bpmh k66dsrZBmc6yVy5VHG9xmhnkO+ZuE3hX1CGHwZVmb5vS6YdCRWj1kVkPn6UsT2ST sEr0U86NBGNsQnIBBADHtYy5FG+BGzIMLCO0J/NxonQlgyUCndjpPmJ3ZSyLj+V5 SuFJ8TMY1GARcsdSkQX4j/1UdHgbjNhEk+w6fHTFwSGR492n/S6ffobmoLTXdkPv AE100GpEti1g7dGG7gyYqH7IPtdYIi1IelRkxX5IbdHwYXu56fMs1IF5x0/azQAR AQABwsCDBBgBCgAPBQJjbEJyBQkPCZwAAhsuAKgJEJR34dBvfze0nSAEGQEKAAYF AmNsQnIACgkQx6i7JWf/QVUzwwQAkPIZlamfe1CbZUuNdTourgkBXy9tSwvTfA3s 4bL8bazSRD6Vbxqs6z7ZmzdLuefJ3UmAGUDLwjjJT0X514K/R8/ao+tJHnGpmEjG VjMCMdBGMCoXRzY615/Y0IzRD3gQrZZjDvtmtZs672STixRQCZan+whd4S23elJu RXuXYP1WbwQA1w95E1YXYw5WgZPApep7XTp9VL6KGfuNQZUFYBHkTyfJAmThPieT NPBEDFGV+QSnDT/7Ijst40hqWmFEz6nihvD6JwNjihrnQ+pBK+yEH3LPLR1HEpJ7 bWtxbkf3RswwxD2huEEHs1QQagCZzLuDM3eqA8Ba6AhMXo8fugAR5BE= =YVN8

-----END PGP PUBLIC KEY BLOCK-----

7. The keys are both .asc files

## Joey Navarrete

CYSE 409: Crime and Computer Applications

11/9/2022

8. Without a passphrase, almost anyone can use the key, so the purpose of the passphrase is to only allow people that know the passphrase to access the keys.

Part 3: Using a real email to send an encrypted message

Primary	Name	Email		Status	Key server	Signatures	
$\checkmark$	Joey Navarret	te joey	nav1107@gmail.com	<ul> <li>valid</li> </ul>	synchronized	1	>
The key da	ita on the Mailvelo	ppe key server is up	to date. Remove all us	er IDs			
Key det	tails				м	<b>1ain Key</b> 6B2B646783837A46	5 🗸
Key det	tails • valid		Key ID	6B2B6467	M 83837A46	4ain Key 6B2B646783837A46	ō V
Key det Status Created	• valid 11/09/2022		Key ID Algorithm	6B2B6467 RSA (Encry	M 83837A46 ypt or Sign)	<b>4ain Key</b> 6B2B646783837A46	ō V
Key det Status Created Expires	valid 11/09/2022 never	Change	Key ID Algorithm Length	6B2B64678 RSA (Energ 4096	M 83837A46 ypt or Sign)	4ain Key 6B2B646783837A46	5 ~

9.

11/9/2022

#### 10. Email: joeynav1107@gmail.com

-----BEGIN PGP PUBLIC KEY BLOCK-----

xsFNBGNsT4gBEADNiHsVlcM6jfz+PTpdNU3KePnpoBvQKctujlVZ+rmOoX1/ NgYTl/KcHRCWIhKd4aG3rJ97iRKVzof1WFf9PAn5WGq25oSfee+HZ8f7/89f xCY1vhpHzKp9B93ZwJS5tCOLJCb4vZSthfXTMANOsv7hlN0BetXM+edigitd 6gieUb3JKMWsb3qGrV4SSz14VY1M4700pgCwaChVtKWYLIggsOMZci9TGFNC EjzbvJRWJdrjb4gK1pogtdT8Kv+HZPobpuMvSc1t7jFh9qFyNJUkbgpmhRab vkZ78P5FS6p18CQ8NVyYrdY+oxnf++j/kWv+PVt8E0LBzLi08sImvbvu8GUP pe82CKcDXzJZ5YkiV1mLJPwbLxAKufpz+KNTn719PwJRN1MARGgq6KgENUNh M5oBzDUYyljuJC9kjQzJ2DK2iDMrqNdMT6NiF5EElRgJjqmF6JtUYSU00ARB toeEcD6VBolBU017Is8dI0w5qeEjTp07d/ple9pSj7sbYmuhF90BOW5/E5Zs ANYdnFDy3y62Dj4U8EIBEAZWkL76U/Vize7hsT2MlzbSEdH9AA7saZ6iOyBU P02Z4VKYa9aEqt7BaCk/p3qQHU9ewgxYo9geULLyrEvLs150qAn7EKOK0h/9 BBr+d4hhEnpS7o0s+6yiqiEQtz2mvv3ofBYCFQARAQABzSZKb2V5IE5hdmFy cmV0ZSA8am9leW5hdjExMDdAZ21haWwuY29tPsLBdQQQAQgAHwUCY2xPiAYL CQcIAwIEFQgKAgMWAgECGQECGwMCHgEACgkQaytkZ40Dekb8nhAAiQ/u6TZ5 HTpezMNkJHBTHJxqoV3Ft+S1SJ+ARli5fbVz5rKJfL8FN1T0+Y6wfy70uCSL RLKOtYmsiDGKQ4ihnOVHQ6cq7KOD63QtCeLgCn0+QuCfzOfeB9EdWc6vYwxt dmAqGrzXYxVeshqcYiBHruCjKwcTO0FpMc7XTw7tBsTDPhQCv1NzxbUAPjr9 E5zTzXQpdqEUr/4ec8VasPHjitFE7d5EviwzOMNkZc1lo6QyEmuoiyCWmrCh sqyAsuGOClBk2gWgG7qekDEZnw29oZqn+7jdn/MtrV5ZXZK1Q9wJSUJz3Z7v +L/iJ6yJ768MspyVZdPoizXb7IOuSvC80BxM0t+ywQBl+k2Kfl7zmnHEbHBI pdbX3hFoCyw39F+1PIV6CbGTCK8WjIJKKBsl+kYQcyjUhxK4E+0VB5mCStuz 3YDCgUnbkHNzl4oOpTPIWG1i6vrdfsh24JvLQ92GB+jMHjNxYwN2LX/oQE7/ 7Ej97G6NXp6vNgIRX6wlqQJbIPn6ndArpML0M9F1+RPYBsu2VJzBckDnMmCX m2o8X751X4tIfGMmgUySM+DdkD7kAsow7yUVvrYI+cS0+nGoQiH+gxW/z7Ws 40UXA0v7QeFh8UnETDVW+WiBVAep56ndy8roUX15ux22+0pp79sqsOrawyIg dSYhYwC0E5AQo9nOwU0EY2xPiAEQALw8UarSDpq0ZNw8TsjEpoxNLhz6Ym5/ 4WXDNpc2x3nwR8VmJ07u0BINXfVolRMQdU0lQUpUL6MudCk4mdIXUVZXzvTz ilTqUXtGtBeUDB6iW85KurA3dxgckSSF6lE+ErIhkaoIMtQnJbGmmkFEulgp axLyRkC/cI1vZ6TXuROORAl1ljKH3X365lQgo1bszpZAPwqGc/PSHrZOq70m e+fCFWRVoP2FYw/R1/MFDAyMYn2NrhS6xWHI/g8IB4xUfGC1Em7JEAwyr5wY qkBL3HSd3S8uIoCRhFzLrDeLGE5PP37cX8131QMhElOG2LbIsa4TqFm4uuii xStuo9Bo1ZN2jEBXNzINslLZmgMJQbJEYuiAB9Lp6cbOo7oD9SLRwya3k9uo xrytF0CgpC0I6p/4EFAokZMMJ9AosefHNt7j0VhG1ezTI4a8fDsA81xr55y9 vGJs9aXA9NPPSGADBp/Y6HrXBdT4U+NXVPM9/Xa4ccojf50Dcx1HHWyiwW98 WYYWY0B6G/LUoTBiFdlCS+c5bk08xihgU4WQ51ftXZ7nvzxCwHCm9I0Y80nq lvHscCEVB8uABpEYY1/n7JSFpylTDazhC/iMVWhfpxMgyofE5e54MnNKUhjr yhwnXGlv1/JLEt0vSQWL9qEEiQHvO5hNe1WMhNCdFfAEhRNIEeu/ABEBAAHC wV8EGAEIAAkFAmNsT4gCGwwACgkQaytkZ40DekZESw//QV611/KAbmdc6NQL IEC9sAs6chXJChcxQ5QU84sUMGk1D8kuVc3pL25Cxc9lEgyp5ARhXarURyzb mrP6uRyg7xRDknT1RRcrXbgMawkLYRX+DalqpArCa94TN3W09kD5TKLrHaUE 8o/lTmVFX8ArkQkFyvO6apymusUxsoY4MncSTLN4/466xZzEtXN9TugqbT+V traEVi2CLqTCL9Sp3t4q2jILz6sVIk5IDPgULLWTMZq2y3eXDdVTrbHViniW Zb4fnp2sU4H+rtCzwdZtno/1YWl3H/AQI5sQgD8HANA+/Ds1oDcrPA4BLCQ4 fULGW/wzkajuS45MwW70dXabEvGcUkEs6p7+Y1Hfi/+NMKQYwT0A3M7TbuFG g5aYFPRGczLz0XPZEt/NwimKv4ZZGACMsHbcHCSWC97W2R/vrLDKY12CWgqp lvphE2oLCR6s5aqivM4Z1G7akxWkzB6HMkBzEYGZhomu+gCaIVUyNUp7X4GV NzmZb53PEciSkoH7GLbs8cVp0t0WlYK30l+TX+B2/4ZfS6nPABUrBpFsub7v 41/FbZ3KFMMXL5/cY+StyNxCJZq8NdTuE0LXIFu16thWMVcmkfVhpuMaI3EX poaaev7FF+nbmPqiNJuakl/uZ5+0ji+wmGAQmXTxtyScQIwvLHNcd7pSpeT8 9eoQSL0=

=o24n

11/9/2022



12. I kept on trying to import the public key, but I would encounter an error saying,

"Invalid no valid key text found." I also tried to send you an email with the public

key, but it would never go through. The best I can do is the image below.

11/9/2022



# 🗉 📷 🐖 🗢 🕥 🔍

13. For a cybersecurity professional, the biggest benefit of asymmetric cryptography is the increase in data security. Since a person will never have to reveal their private key, along with having a passphrase, it is one of the most secure ways that data can

## Joey Navarrete

CYSE 409: Crime and Computer Applications

11/9/2022

be protected. Another advantage of using asymmetric cryptography is that keys don't need to be exchanged.

Using asymmetric cryptography also allows the person that is receiving the message to verify its origin. Someone who is a cybersecurity professional may be trying to send data to another source, and with it being encrypted asymmetrically, they should not have to worry about anyone gaining access to that data except for the person that is receiving the data.