Jurnal Kreativa: Kemitraan Responsif untuk Aksi Inovasi dan Pengabdian Masyarakat
E-ISSN: 3024-9236; P-ISSN: 3026-7323
Journal Homepage: http://journal.lontaradigitech.com/KREATIVA

Python dan Kriptografi: Edukasi dan Pengabdian untuk Masa Depan yang Aman

Muhammad Fajar B[1*], Abdul Wahid[2], Gufran Darma Dirawan[3], M Syahid Nur Wahid[4], Andi Akram Nur Risal[5]

[1,5]*Program Studi Teknik Komputer, Universitas Negeri Makassar, Indonesia*
[2]*Program Studi Pendidikan Bahasa dan Sastra Indonesia, Universitas Negeri Makassar, Indonesia*
[3]*Program Studi Pendidikan Kependudukan dan Lingkungan Hidup Universitas Negeri Makassar, Indonesia*
[4]*Program Studi Pendidikan Teknik Informatika dan Komputer, Universitas Negeri Makassar, Indonesia*

Email: fajarb@unm.ac.id[1], wahid@unm.ac.id[2], syahid@unm.ac.id[3], andi.akram@unm.ac.id[4], gufran.darma@unm.ac.id[5]

INFO ARTIKEL
Kata kunci:
Kriptografi, *Python*, *Symmetric Cryptography*, *Asymmetric Cryptography*, *Hash Function*

ABSTRAK
Di era digital, keamanan data menjadi krusial, dan integrasi *Python* dengan kriptografi muncul sebagai solusi efektif untuk masa depan yang aman. *Python*, dengan kesederhanaan sintaks dan pustaka kaya seperti *NumPy* dan *SciPy*, menjadi alat ideal untuk pemula dan aplikasi kriptografi. Workshop ini diadakan untuk memberikan pemahaman tentang kriptografi dan aplikasinya menggunakan *Python*. Materi mencakup dasar-dasar kriptografi, algoritma seperti AES dan RSA, serta praktik langsung implementasi enkripsi dan dekripsi. Melalui latihan praktis, peserta dapat menjembatani teori dan aplikasi, memperkuat kemampuan pemecahan masalah yang diperlukan untuk menghadapi ancaman keamanan dunia nyata. Hasil evaluasi menunjukkan peningkatan pemahaman konsep kriptografi dan keterampilan praktis peserta, yang diukur melalui kuis dan tes praktik. Feedback positif menunjukkan kepuasan terhadap materi dan penyelenggaraan workshop. Kegiatan ini tidak hanya meningkatkan pengetahuan teknis, tetapi juga menumbuhkan kesadaran tentang pentingnya keamanan informasi, berkontribusi pada ekosistem digital yang lebih aman. Program ini menyarankan pengembangan lebih lanjut dengan cakupan materi lebih luas untuk terus mendukung pendidikan dan pengembangan keterampilan keamanan data mahasiswa, mempersiapkan mereka untuk tantangan keamanan siber di masa depan.

1. PENDAHULUAN

Di era digital, keamanan data merupakan hal yang sangat penting, dan integrasi pemrograman *Python* dengan kriptografi muncul sebagai alat yang kuat untuk memastikan masa depan yang aman. *Python* dikenal dengan fleksibilitas dan keramahannya, digunakan secara luas di berbagai bidang, termasuk kriptografi (Zhang, 2023).

* Penulis Korespondensi: Muhammad Fajar B

Diterima 3 Januari 2024; Disetujui 31 Januari 2024
Tersedia secara daring 31 Januari 2024
Dipublikasikan oleh *Lontara Digitech Indonesia*

Kesederhanaan sintaks python membuatnya menjadi pilihan yang sangat baik untuk pemula, memungkinkan mereka untuk memahami konsep pemrograman dengan cepat dan menerapkannya secara efektif (Feng, 2021). Selain itu, pustaka *Python* yang kaya, seperti *NumPy* dan *SciPy*, menawarkan dukungan yang kuat untuk komputasi ilmiah, menjadikan aset yang berharga dalam aplikasi kriptografi (Weiss, 2017). Paparan awal terhadap *Python*, terutama dalam konteks kriptografi, membekali siswa dengan keterampilan penting untuk mengatasi tantangan keamanan yang rumit (Mariano et al., 2019).

Kriptografi, praktik komunikasi yang aman, merupakan hal yang mendasar bagi keamanan informasi (González-Tablas et al., 2020). Melalui teknik kriptografi, data sensitif dapat dilindungi dari akses dan gangguan yang tidak sah, memastikan kerahasiaan dan integritas (Xu et al., 2009). Memasukkan *Python* ke dalam pendidikan kriptografi tidak hanya meningkatkan kemampuan pemrograman siswa tetapi juga memperdalam pemahaman mereka tentang prinsip-prinsip kriptografi (Yong et al., 2017). Melibatkan siswa dalam latihan praktis yang melibatkan implementasi algoritma kriptografi dalam *Python* membantu menjembatani kesenjangan antara teori dan aplikasi, mendorong pengalaman belajar yang komprehensif (Deeb & Hickey, 2019). Pendekatan langsung ini memperkuat konsep teoretis dan menumbuhkan kemampuan pemecahan masalah yang sangat penting untuk mengatasi ancaman keamanan di dunia nyata.

Sinergi antara *Python* dan kriptografi meluas di luar pengaturan pendidikan hingga aplikasi praktis dalam keamanan siber. Alat-alat seperti *Cyber Security Tool Kit* (CyberSecTK), yang dikembangkan menggunakan *Python*, merupakan contoh kolaborasi antara pemrograman dan keamanan (Calix et al., 2020). Inisiatif tersebut sejalan dengan klaim *Python* dalam menangani beragam tugas keamanan siber, mulai dari pemrosesan data hingga pembelajaran mesin (Mankovskyy, 2024). Selain itu, kemunculan jaringan kriptografi kuantum menunjukkan evolusi sistem komunikasi yang aman, memanfaatkan teknologi canggih di samping kerangka kerja pemrograman yang kuat (Xu et al., 2009). Adaptasi dan skalabilitas *Python* membuatnya menjadi pilihan yang lebih disukai untuk mengimplementasikan solusi kriptografi yang kompleks yang memenuhi tuntutan tantangan keamanan siber modern.

Dalam ranah layanan masyarakat, inisiatif yang mempromosikan pendidikan *Python* dan kriptografi memainkan peran penting dalam memberdayakan individu dengan pengetahuan dan keterampilan untuk melindungi aset digital (López-Incera et al., 2020). Dengan menyelenggarakan lokakarya, seminar, dan program penjangkauan yang berfokus pada *Python* dan kriptografi, komunitas dapat meningkatkan kesadaran tentang ancaman keamanan siber dan pentingnya enkripsi (Wang et al., 2020). Upaya kolaboratif yang menyatukan pendidik, siswa, dan penggemar teknologi dapat menumbuhkan budaya kesadaran keamanan siber, meletakkan dasar bagi ekosistem digital yang lebih aman (Kuhail et al., 2022). Selain itu, mengintegrasikan pendekatan lain ke dalam pendidikan kriptografi dapat meningkatkan pengalaman belajar, membuatnya menarik dan interaktif untuk audiens yang lebih luas (Deeb & Hickey, 2019; González-Tablas et al., 2020).

Menyadari pentingnya penguasaan teknologi kriptografi bagi para profesional keamanan di masa depan, program edukasi dan pengabdian masyarakat dengan tema "*Python* dan Kriptografi: Edukasi dan Pengabdian untuk Masa Depan yang Aman" diadakan untuk mahasiswa. Kegiatan ini bertujuan untuk memberikan pemahaman mendalam tentang prinsip-prinsip dasar kriptografi serta penerapannya menggunakan bahasa pemrograman *Python*.

Pengabdian ini tidak hanya bertujuan untuk meningkatkan pengetahuan teknis para mahasiswa, tetapi juga untuk mempersiapkan mereka dalam menghadapi tantangan keamanan siber di dunia nyata. Dengan menguasai kriptografi dan aplikasi praktisnya melalui *Python*, mahasiswa diharapkan dapat berkontribusi secara signifikan dalam menjaga keamanan data dan informasi di berbagai sektor. Tidak hanya itu, kegiatan ini juga bertujuan untuk membangun kesadaran akan pentingnya keamanan informasi di kalangan akademisi dan masyarakat luas. Dengan penyebaran pengetahuan yang tepat, diharapkan akan tercipta lingkungan digital yang lebih aman dan terlindungi dari berbagai ancaman siber.

Melalui kegiatan edukasi dan pengabdian ini, mahasiswa diajak untuk berkolaborasi, berbagi pengetahuan, dan mengembangkan solusi inovatif dalam bidang kriptografi. Dengan demikian, program ini diharapkan dapat mencetak generasi muda yang tidak hanya ahli dalam bidang teknis, tetapi juga memiliki kesadaran tinggi akan pentingnya keamanan informasi di era digital.

Berdasarkan hasil observasi dan urgensi mengenai keamanan data, integrasi pemrograman *Python* dengan kriptografi tidak hanya memperkaya pengalaman pendidikan mahasiswa sarjana teknik komputer, tetapi juga memberdayakan mereka untuk berkontribusi secara bermakna dalam bidang keamanan siber. Dengan membekali mahasiswa dengan alat dan pengetahuan untuk menavigasi seluk-beluk komunikasi yang aman, inisiatif *Python* dan kriptografi membuka jalan bagi masa depan yang lebih tangguh dan aman, di mana generasi profesional teknik komputer berikutnya dapat secara efektif mengatasi tantangan keamanan data yang terus berkembang.

2. METODE PELAKSANAAN

Pengabdian kepada Masyarakat ini dilaksanakan melalui serangkaian tahapan seperti yang disajikan pada Gambar 1 berikut:

Gambar 1. Tahapan Pelaksanaan

a. Persiapan
Tahap persiapan dilakukan untuk memastikan semua aspek kegiatan siap sebelum pelaksanaan workshop. Aktivitas yang dilakukan pada tahap ini meliputi:
1) Penyusunan Materi: Tim pengabdian menyusun materi yang akan dipresentasikan. Materi mencakup pengenalan kriptografi, dasar-dasar teori kriptografi, algoritma kriptografi, dan implementasi kriptografi menggunakan bahasa pemrograman *Python*.
2) Koordinasi dengan Pihak Fakultas: Tim mengadakan pertemuan dengan pihak Fakultas Sains dan Teknologi UIN Alauddin Makassar untuk membahas kebutuhan logistik, peralatan, dan ruangan yang akan digunakan.
3) Penyediaan Peralatan dan Materi Pendukung: Menyiapkan peralatan yang dibutuhkan seperti laptop, proyektor, dan perangkat jaringan.

b. Pemaparan Materi
Tahap ini merupakan bagian awal dari pelaksanaan workshop, yang dilakukan dengan tujuan memberikan pemahaman dasar kepada peserta mengenai kriptografi dan implementasinya dengan *Python*. Kegiatan pada tahap ini meliputi:
1) Pembukaan dan Sambutan: Kegiatan diawali dengan pembukaan oleh ketua tim pengabdian dan sambutan dari perwakilan fakultas.
2) Pemaparan Teori Kriptografi: Materi yang dipaparkan mencakup sejarah kriptografi, konsep dasar kriptografi, dan jenis-jenis algoritma kriptografi seperti enkripsi simetris dan asimetris.

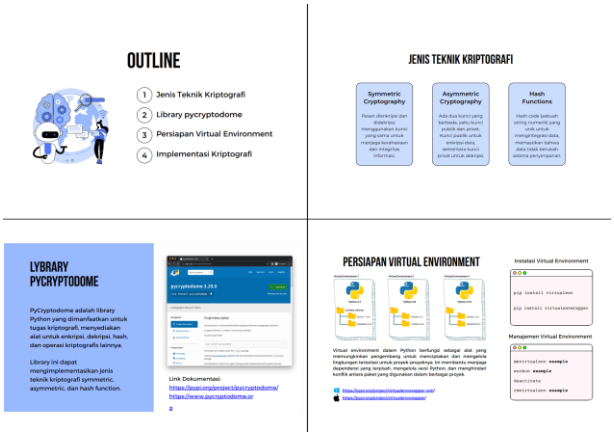
3) Pengenalan *Python* untuk Kriptografi: Peserta diperkenalkan pada bahasa pemrograman *Python*, termasuk instalasi, penggunaan dasar, dan pustaka-pustaka yang relevan untuk kriptografi seperti *PyCryptoDome*.

c. Workshop
Rangkaian kegiatan pada tahap ini meliputi:
1) Praktik Implementasi Kriptografi dengan *Python*: Peserta diajak untuk langsung mempraktikkan implementasi algoritma kriptografi menggunakan *Python*. Materi praktik mencakup enkripsi dan dekripsi pesan, penggunaan kunci publik dan kunci pribadi, serta penerapan digital *signature*.
2) Studi Kasus: Peserta diberikan studi kasus nyata terkait keamanan data yang harus dipecahkan menggunakan teknik kriptografi yang telah dipelajari.
3) Diskusi dan Tanya Jawab: Sesi diskusi dibuka untuk memberikan kesempatan kepada peserta bertanya mengenai kesulitan atau kebingungan yang dihadapi selama praktik.

d. Evaluasi
Tahap evaluasi dilakukan untuk mengukur keberhasilan kegiatan dan pemahaman peserta terhadap materi yang telah disampaikan. Aktivitas evaluasi meliputi:
1) Kuis dan Tes Praktik: Peserta diberikan kuis dan tes praktik untuk mengukur pemahaman mereka terhadap teori dan implementasi kriptografi menggunakan *Python*.
2) *Feedback* dari Peserta: Pengumpulan *feedback* dari peserta dilakukan melalui kuesioner yang mencakup aspek kepuasan terhadap penyelenggaraan kegiatan, kualitas materi, dan manfaat yang dirasakan.
3) Analisis dan Pelaporan: Tim pengabdian menganalisis hasil kuis, tes praktik, dan *feedback* untuk menyusun laporan akhir kegiatan. Laporan ini berisi evaluasi keseluruhan kegiatan, pencapaian tujuan, serta rekomendasi untuk kegiatan serupa di masa mendatang.

3. HASIL DAN PEMBAHASAN

Workshop dilaksanakan pada hari Sabtu, 21 Oktober 2023, dan diikuti oleh sekitar 73 mahasiswa. Kegiatan workshop berlangsung di ruang Lab Pemrograman Lanjutan 403-406 Fakultas Sains dan Teknologi UIN Alauddin Makassar. Kegiatan Workshop diawali dengan pemaparan materi kepada peserta. Gambar 2 berikut adalah tangkapan layar bahan tayang yang disajikan kepada peserta:



Gambar 2. Tangkapan Layar Bahan Tayang

Pada pemaparan materi yang disajikan terdiri dari beberapa pembahasan yakni dimulai dari Jenis Teknik Kriptografi, pustaka *pycrytodome*, persiapan *virtual environment*, hingga implementasi kriptografi yang disajikan sebagai persiapan praktikum langsung. Adapun materi workshop yang diberikan kepada peserta yang dalam hal ini adalah mahasiswa, di antaranya *Advanced Encryption Standard* (AES), Algoritme *Rivest Shamir Aldeman* (RSA), Algoritme *Hybrid*, Algoritma SHA-256.

Berikut adalah salah satu *script* kode *python* untuk mengimplementasikan algoritme AES:

1) Enkripsi

```python
from Crypto.Cipher import AES
from Crypto.Random import get_random_bytes

data = b'secret data'

key = get_random_bytes(16)
print(key)
cipher = AES.new(key, AES.MODE_EAX)
ciphertext, tag = cipher.encrypt_and_digest(data)

file_out = open("encrypted.bin", "wb")
[ file_out.write(x) for x in (cipher.nonce, tag, ciphertext) ]
file_out.close()
```

Gambar 3. Tangkapan Layar *Script* Kode Enkripsi (AES)

2) Dekripsi

```python
from Crypto.Cipher import AES

file_in = open("encrypted.bin", "rb")
nonce, tag, ciphertext = [ file_in.read(x) for x in (16, 16, -1) ]
file_in.close()

# let's assume that the key is somehow available again
cipher = AES.new(b'R\xf0\xeb\xb4!t5\xf9mY\xc7\x04?\xea\xca8', AES.MODE_EAX, nonce)
data = cipher.decrypt_and_verify(ciphertext, tag)
print(data)
```

Gambar 4. Tangkapan Layar *Script* Kode Dekripsi (AES)

Gambar 3 merupakan *script* kode *Python* yang digunakan untuk enkripsi data menggunakan AES. Terlihat beberapa langkah utama, termasuk pembuatan kunci enkripsi, inisialisasi *cipher*, enkripsi data, dan penyimpanan hasil enkripsi ke dalam file biner. Dengan memahami setiap bagian dari *script* ini, mahasiswa dapat belajar bagaimana menerapkan enkripsi AES secara praktis dan aman, serta memahami pentingnya setiap komponen dalam proses enkripsi.

Gambar 4 merupakan *script* kode *Python* yang digunakan untuk dekripsi data menggunakan AES. Terlihat beberapa langkah utama, termasuk pembacaan *nonce*, *tag*, dan *ciphertext* dari file, inisialisasi *cipher* dengan kunci dan *nonce*, serta dekripsi dan verifikasi data. Dengan memahami setiap bagian dari *script* ini, mahasiswa dapat belajar bagaimana proses dekripsi bekerja dan pentingnya menjaga kunci enkripsi tetap aman.

Selama sesi workshop, peserta diberikan kesempatan untuk langsung mempraktikkan pengetahuan yang telah mereka dapatkan. Mereka melakukan implementasi algoritma enkripsi dan dekripsi sederhana, menggunakan pustaka *Python* seperti *PyCryptodome*. Hasil praktik

menunjukkan bahwa sebagian besar peserta mampu mengikuti instruksi dengan baik dan berhasil menyelesaikan tugas-tugas yang diberikan. Studi kasus yang disajikan dalam workshop juga memberikan gambaran nyata tentang aplikasi kriptografi dalam menjaga keamanan data, sehingga peserta mendapatkan wawasan yang lebih komprehensif. Gambar 5 dan 6 berikut adalah dokumentasi dari kegiatan pelatihan yang dilakukan:

Gambar 5. Dokumentasi Kegiatan (1)

Gambar 6. Dokumentasi Kegiatan (2)

Evaluasi dilakukan melalui kuis dan tes praktik yang dirancang untuk mengukur pemahaman peserta. Hasil evaluasi menunjukkan bahwa mayoritas peserta memiliki pemahaman yang baik tentang konsep-konsep dasar kriptografi dan mampu mengaplikasikannya dalam pemrograman *Python*. Selain itu, *feedback* dari peserta yang dikumpulkan melalui kuesioner menunjukkan tingkat kepuasan yang tinggi terhadap penyelenggaraan kegiatan, kualitas materi, serta penyampaian oleh pemateri. Peserta juga mengapresiasi kesempatan untuk terlibat dalam praktik langsung, yang menurut mereka sangat membantu dalam memahami materi secara lebih mendalam.

Secara keseluruhan, kegiatan ini berhasil mencapai tujuannya dalam memberikan edukasi mengenai kriptografi dan implementasinya menggunakan *Python*. Kegiatan ini tidak hanya meningkatkan pemahaman peserta mengenai pentingnya keamanan data, tetapi juga memberikan keterampilan praktis yang dapat mereka aplikasikan dalam studi dan pekerjaan di masa depan. Rekomendasi dari kegiatan ini adalah agar program serupa dapat terus dilakukan dengan cakupan yang lebih luas, serta materi yang lebih mendalam untuk tingkat lanjutan.

Dengan demikian, kegiatan pengabdian masyarakat seperti ini dapat berkontribusi lebih signifikan dalam menciptakan sumber daya manusia yang kompeten di bidang keamanan data.

4. KESIMPULAN

Kegiatan pengabdian masyarakat bertema "*Python* dan Kriptografi: Edukasi dan Pengabdian untuk Masa Depan yang Aman" telah dilaksanakan dengan sukses, menghasilkan berbagai pencapaian positif yang signifikan. Kegiatan ini berhasil meningkatkan pemahaman teori kriptografi dan kemampuan implementasi praktis menggunakan *Python* di kalangan mahasiswa, yang terlihat dari peningkatan nilai rata-rata kuis dan keberhasilan dalam tes praktik. Metode pengajaran yang menggabungkan pemaparan teori dengan praktik langsung terbukti efektif dalam membantu peserta memahami konsep kriptografi dan menerapkannya, sementara studi kasus dan diskusi interaktif turut berkontribusi positif terhadap proses pembelajaran. Partisipasi yang tinggi dan *feedback* positif dari peserta mencerminkan antusiasme besar terhadap topik ini, menunjukkan relevansi dan pentingnya kriptografi dan *Python* di kalangan mahasiswa yang berkonsentrasi pada keamanan data. Dengan keterampilan baru yang diperoleh, peserta siap untuk menerapkan teknik kriptografi dalam berbagai situasi nyata, baik dalam studi lanjut maupun di dunia kerja, yang diharapkan dapat meningkatkan keamanan data dan teknologi yang lebih aman di masa depan. Berdasarkan hasil yang dicapai, disarankan untuk mengadakan kegiatan serupa secara berkala dan memperluas topik yang dibahas untuk memberikan kesempatan lebih banyak kepada mahasiswa dalam mendalami berbagai aspek keamanan data dan teknologi terkait. Secara keseluruhan, kegiatan ini tidak hanya memberikan pengetahuan teoretis tetapi juga keterampilan praktis yang berguna bagi para peserta, sehingga mereka lebih siap menghadapi tantangan di bidang keamanan data dan berkontribusi pada pengembangan teknologi yang aman dan terpercaya di masa depan.

REFERENSI

Calix, R., Singh, S., Chen, T., Zhang, D., & Tu, M. (2020). Cyber security tool kit (cybersectk): a python library for machine learning and cyber security. Information, 11(2), 100. https://doi.org/10.3390/info11020100

Deeb, F. and Hickey, T. (2019). Teaching introductory cryptography using a 3d escape-the-room game.. https://doi.org/10.1109/fie43999.2019.9028549

Feng, G. (2021). Reform and practice of mixed teaching in the course of python programming. Academic Journal of Computing & Information Science, 4(1). https://doi.org/10.25236/ajcis.2021.040113

González-Tablas, A., Vasco, M., Cascos, I., & Palomino, Á. (2020). Shuffle, cut, and learn: crypto go, a card game for teaching cryptography. Mathematics, 8(11), 1993. https://doi.org/10.3390/math8111993

Kuhail, M., Mathew, S., Hammad, R., & Bahja, M. (2022). Blockchain primer., 28-47. https://doi.org/10.4018/978-1-7998-8382-1.ch003

López-Incera, A., Hartmann, A., & Dür, W. (2020). Encrypt me! a game-based approach to bell inequalities and quantum cryptography. European Journal of Physics, 41(6), 065702. https://doi.org/10.1088/1361-6404/ab9a67

Mankovskyy, S. (2024). Python model of secret key agreement in the group of arbitrary number of participants. Information and Communication Technologies Electronic Engineering, 4(1), 93-101. https://doi.org/10.23939/ictee2024.01.093

Mariano, D., Martins, P., Santos, L., & Minardi, R. (2019). Introducing programming skills for life science students. Biochemistry and Molecular Biology Education, 47(3), 288-295. https://doi.org/10.1002/bmb.21230

Wang, S., Liu, D., Wang, N., & Yuan, Y. (2020). Design and implementation of an online python teaching case library for the training of application-oriented talents. International Journal of Emerging Technologies in Learning (Ijet), 15(21), 217. https://doi.org/10.3991/ijet.v15i21.18191

Weiss, C. (2017). Scientific computing for chemists: an undergraduate course in simulations, data processing, and visualization. Journal of Chemical Education, 94(5), 592-597. https://doi.org/10.1021/acs.jchemed.7b00078

Xu, F., Chen, W., Wang, S., Yin, Z., Zhang, Y., Liu, Y., … & Guo, G. (2009). Field experiment on a robust hierarchical metropolitan quantum cryptography network. Chinese Science Bulletin, 54(17), 2991-2997. https://doi.org/10.1007/s11434-009-0526-3

Yong, W., Hill, K., & Foley, E. (2017). Computer programming with python for industrial and systems engineers: perspectives from an instructor and students. Computer Applications in Engineering Education, 25(5), 800-811. https://doi.org/10.1002/cae.21837

Zhang, Z. (2023). Analysis of large data sets in a physical chemistry laboratory nmr experiment using python. Journal of Chemical Education, 100(10), 4109-4113. https://doi.org/10.1021/acs.jchemed.3c00586