Jan 16, 2026

Decryption of genome-encoded cryptographic keys using DNAcrypt-AI

DOI
https://dx.doi.org/10.17504/protocols.io.5qpvo1387g4o/v1

Marvin De los Santos[1], Chikie Lynn[1]

[1]ChordexBio

Marvin De los Santos
ChordexBio

DOI: https://dx.doi.org/10.17504/protocols.io.5qpvo1387g4o/v1

Protocol Citation: Marvin De los Santos, Chikie Lynn 2026. Decryption of genome-encoded cryptographic keys using DNAcrypt-AI. **protocols.io** https://dx.doi.org/10.17504/protocols.io.5qpvo1387g4o/v1

Protocol status: Working
We use this protocol and it's working

Created: January 16, 2026

Last Modified: January 16, 2026

Protocol Integer ID: 238788

Keywords: DNAcrypt-AI, FAS2rDNA, Covary, ChordexBio, DNA-based cryptography, human genome, k-mer encoding, sequence-based decryption, secret key recovery, genome metadata, DNA sequence reconstruction, programmable biology, bioinformatics security, synthetic DNA computing, machine learning-assisted decryption, cloud-based computational workflow, Jupyter Notebook, Google Colab, decryption of genome, ai dnacrypt, dnacrypt, throughput dna sequence reconstitution pipeline, encrypted genome coordinate, reproducible reversibility of the dnacrypt, using dnacrypt, decryption cycle for research, decryption, controlled decryption, decryption workflow, genome metadata representation, ai encryption, decryption cycle, genome, decryption of encrypted digital credential, readable secret key, encoded cryptographic key, encrypted secret key, character secret key, secret key, genome vocabulary, sequence intelligence model, cryptographic key, genome coordinate, encrypted digital credential, sequence reconstruction, length plaintext key, b

Disclaimer

Abstract

DNAcrypt-AI is a human genome-based cryptographic framework that leverages k-mer-based alphanumeric encoding, genome vocabulary, sequence reconstruction, and sequence-informed machine learning to enable controlled decryption of encrypted digital credentials. This protocol describes the procedure for decrypting an encrypted secret key generated using DNAcrypt-AI, restoring the original fixed-length plaintext key from its genome metadata representation. The decryption workflow is implemented on Google Colab and integrates a high-throughput DNA sequence reconstitution pipeline (FAS2rDNA) with a sequence intelligence model (Covary) to reconstruct the encrypted genome coordinates into a human-readable secret key. The protocol successfully recovered the expected 16-character secret key, demonstrating reproducible reversibility of the DNAcrypt-AI encryption-decryption cycle for research and educational use.

Before start

For this protocol to work, users must generate and encrypt a 16-character secret key using DNAcrypt-AI (see protocol here: **10.17504/protocols.io.14egn12k6v5d/v1**. Save and store the DNAcrypt_metadata.json file, which is the genome-encrypted data, and will be used for the decryption exercise. DNAcrypt-AI is implemented as a Jupyter notebook that is hosted on Google Colab. DNAcrypt-AI is dependent on a high-throughput DNA sequence reconstitution pipeline (**FAS2rDNA**) and sequence-informed machine learning model (**Covary**).

Protocol procedure

1 Launch DNAcrypt-AI from **https://dnacryptai.chordexbio.com/**. Alternatively, you can run DNAcrypt-AI using the recommended methods described in https://github.com/mahvin92/DNAcrypt-AI.

2 Select 'Decryption' under the *Use cases* section in the user configuration interface, as shown in Figure 1 below.

Figure 1. The interface of user configuration on DNAcrypt-AI, where users can specify the behavior of the cipher.

3 Run DNAcrypt-AI by initiating a runtime, ensuring a GPU (T4 as default) support, if available. Note that DNAcrypt-AI will still work in a non-GPU hosted runtime.

```
Click "Runtime" -> Select "Run all"
```

4 Upload the previously generated genome-encrypted data (see *Before starting*), using the upload feature as shown in Figure 2 below.

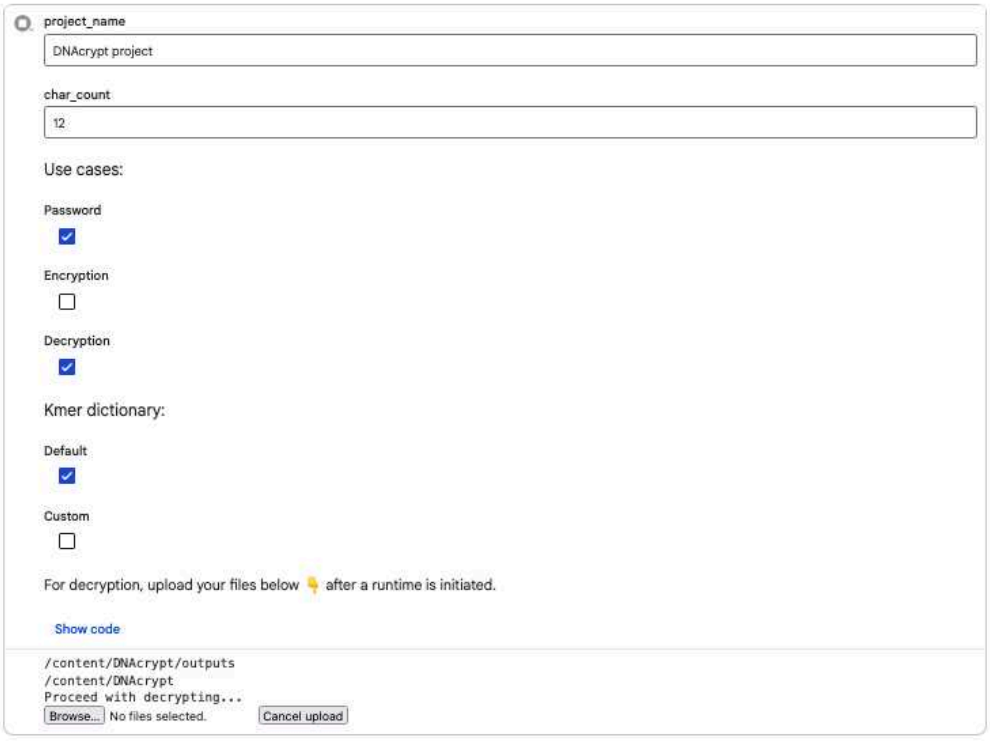

Figure 2. The upload functionality on DNAcrypt-AI Jupyter notebook, executed in Google Colab environment.

5 Wait for DNAcrypt-AI to finish the decryption process. The status and any error will be displayed below the code cell.

6 The decrypted 16-character key will be displayed below the code cell. Note that if you generated and encrypted a key with length from 6 to 90 characters, DNAcrypt-AI will yield a key with the same character length.

Application note

7 This protocol is designed for decrypting passwords or encrypted keys, which are originally encoded into genome coordinated (encrypted data) by DNAcrypt-AI. Decryption relies on correct metadata and compatible k-mer encoding logic, ensuring controlled reversibility of the cipher. This workflow is intended for research, validation, and educational use cases involving DNA-based cryptographic systems.