

KOMBINASI CAESAR CIPHER, VIGENÈRE CIPHER, DAN VIGENÈRE AUTOKEY PADA APLIKASI WEB CATATAN HARIAN UNTUK MENINGKATKAN KEAMANAN PENYIMPANAN DATA

- 1.Muhammad Arifin Sulistiono - 20230801095
- 2.Alfin Khalaj Syahruwardi - 20230801465
- 3.Fitra Candra Ramadhani - 20230801202

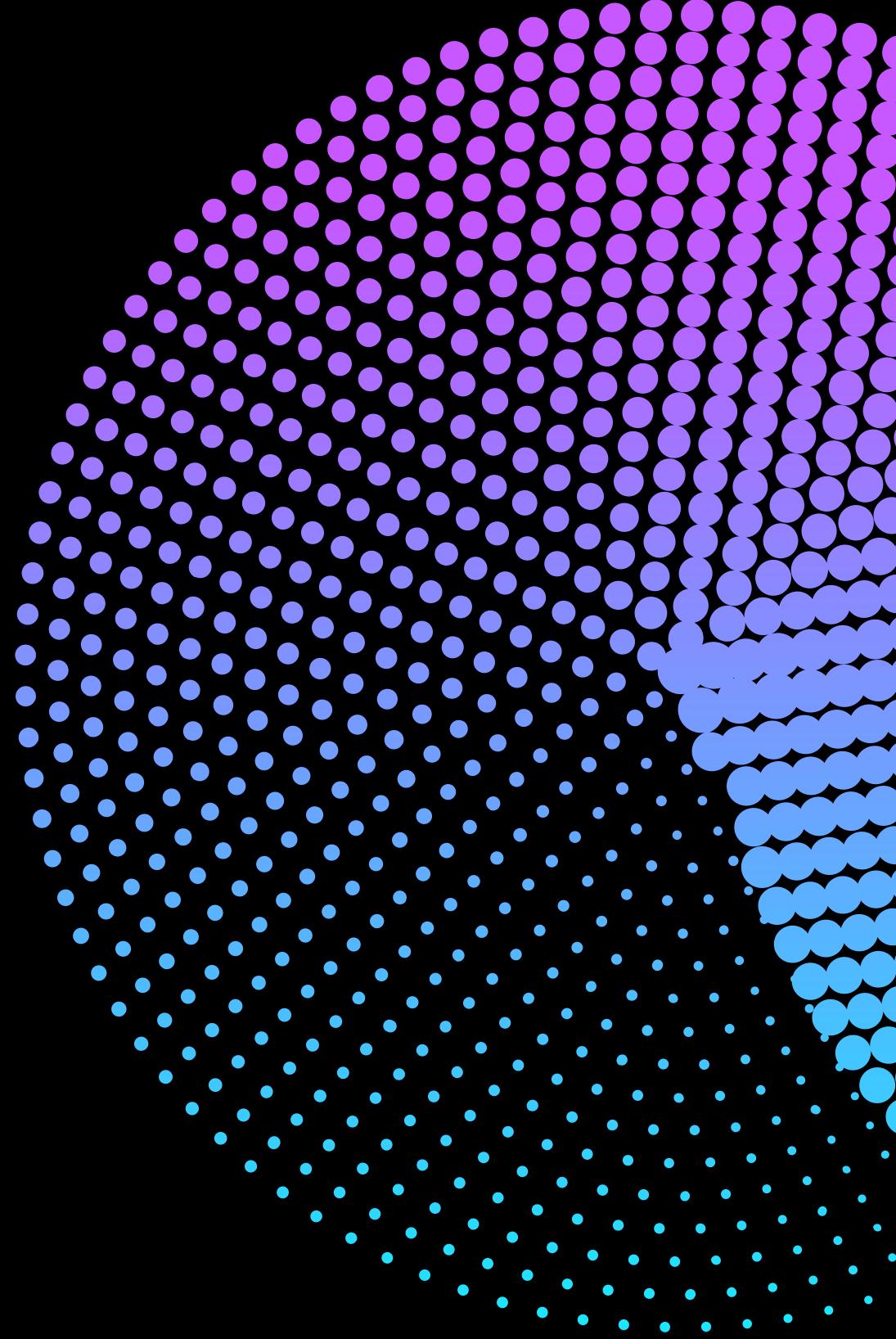
2

Latar Belakang Penelitian

Keamanan penyimpanan data teks menjadi kebutuhan penting seiring meningkatnya ancaman keamanan siber terhadap informasi digital, baik milik individu maupun organisasi. Data seperti catatan harian memiliki nilai privasi tinggi sehingga memerlukan perlindungan khusus agar tidak dapat diakses oleh pihak yang tidak berwenang.

Kriptografi merupakan salah satu teknik utama dalam menjaga kerahasiaan data. Meskipun kriptografi modern telah banyak diterapkan, kriptografi klasik masih digunakan karena memiliki keunggulan dalam hal kesederhanaan dan efisiensi komputasi. Namun, algoritma klasik seperti Caesar Cipher dan Vigenère Cipher jika digunakan secara tunggal memiliki kelemahan, terutama terhadap serangan analisis frekuensi.

Oleh karena itu, penelitian ini mengkaji penerapan kombinasi beberapa algoritma kriptografi klasik sebagai bentuk super enkripsi untuk meningkatkan keamanan penyimpanan data teks tanpa menambah beban komputasi yang signifikan.



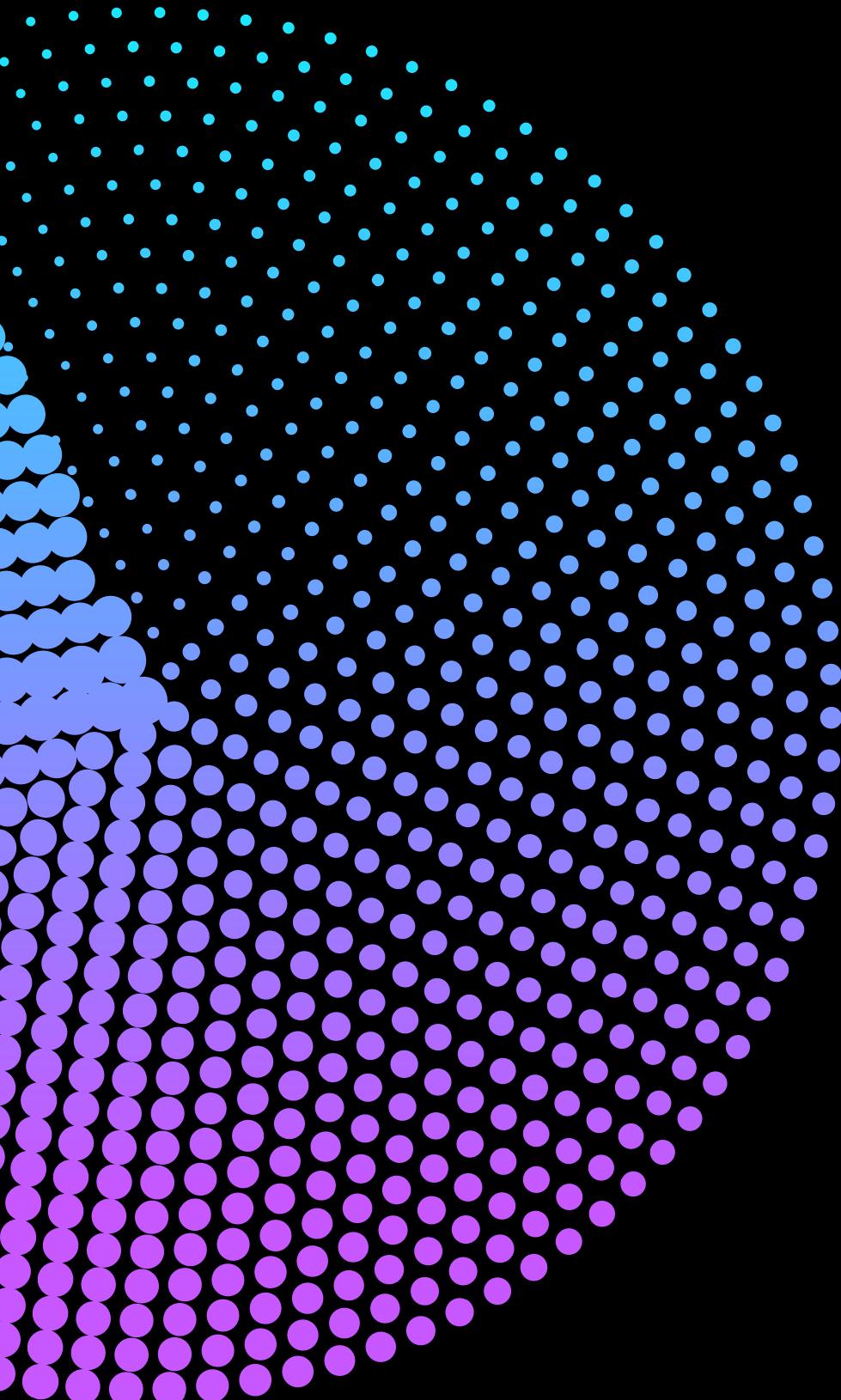


Konsep dan Metode Penelitian

Penelitian ini menggunakan metode studi literatur dengan pendekatan deskriptif-analitis, yaitu dengan mengkaji dan menganalisis berbagai penelitian terdahulu yang membahas kombinasi algoritma kriptografi klasik. Fokus utama penelitian adalah pada penerapan Caesar Cipher, Vigenère Cipher, dan varian Vigenère Autokey dalam satu skema enkripsi berlapis.

Caesar Cipher merupakan algoritma substitusi monoalfabetik yang menggunakan pergeseran karakter tetap, sedangkan Vigenère Cipher adalah substitusi polialfabetik yang menggunakan kunci berulang. Untuk mengatasi kelemahan perulangan kunci, digunakan Vigenère Autokey yang memanfaatkan plaintext sebagai bagian dari kunci.

Kombinasi algoritma ini dikenal sebagai super enkripsi atau product cipher, di mana proses enkripsi dilakukan secara berurutan dengan tujuan meningkatkan tingkat confusion dan diffusion pada data.



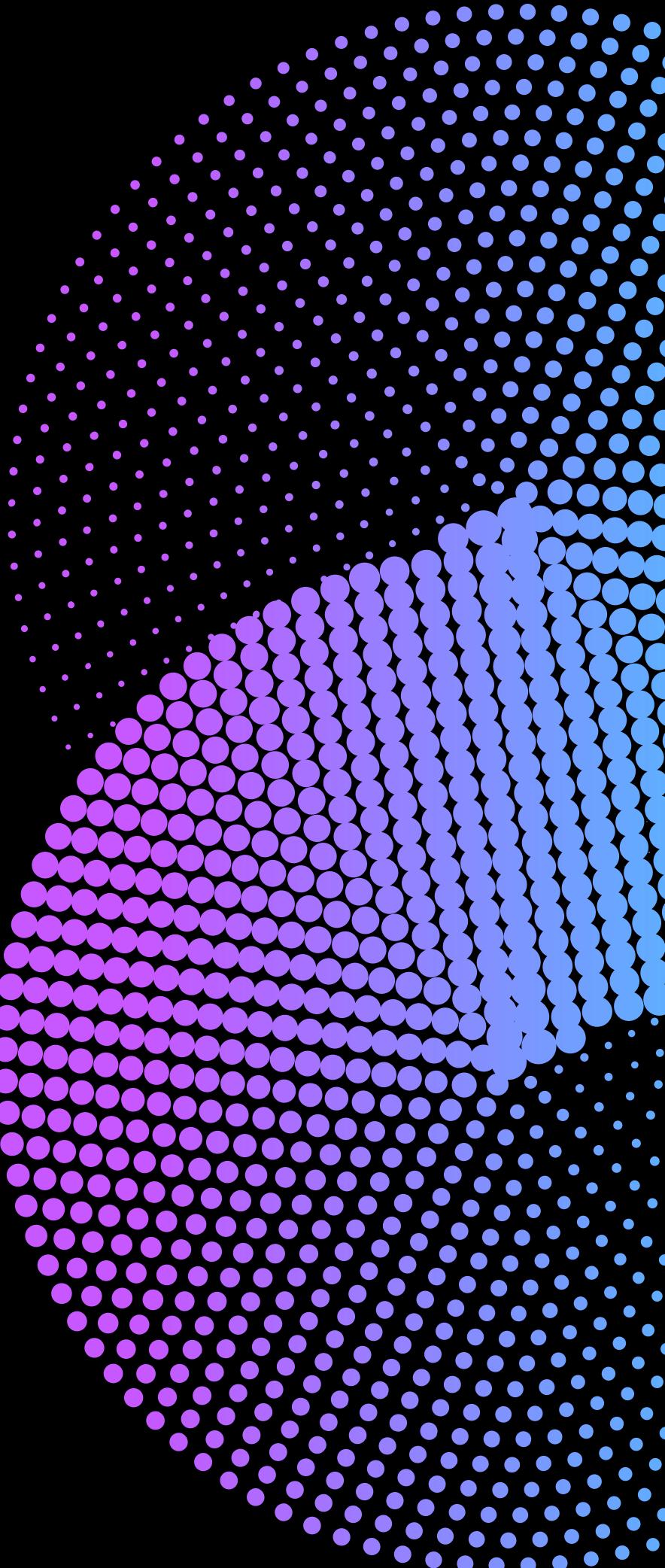
4

Hasil dan Analisis Keamanan

Hasil analisis dari penelitian terdahulu menunjukkan bahwa penerapan kombinasi Caesar Cipher dan Vigenère Autokey mampu meningkatkan tingkat keamanan data secara kuantitatif. Hal ini dibuktikan melalui pengukuran nilai entropi ciphertext yang mengalami peningkatan dibandingkan penggunaan algoritma Caesar Cipher secara tunggal.

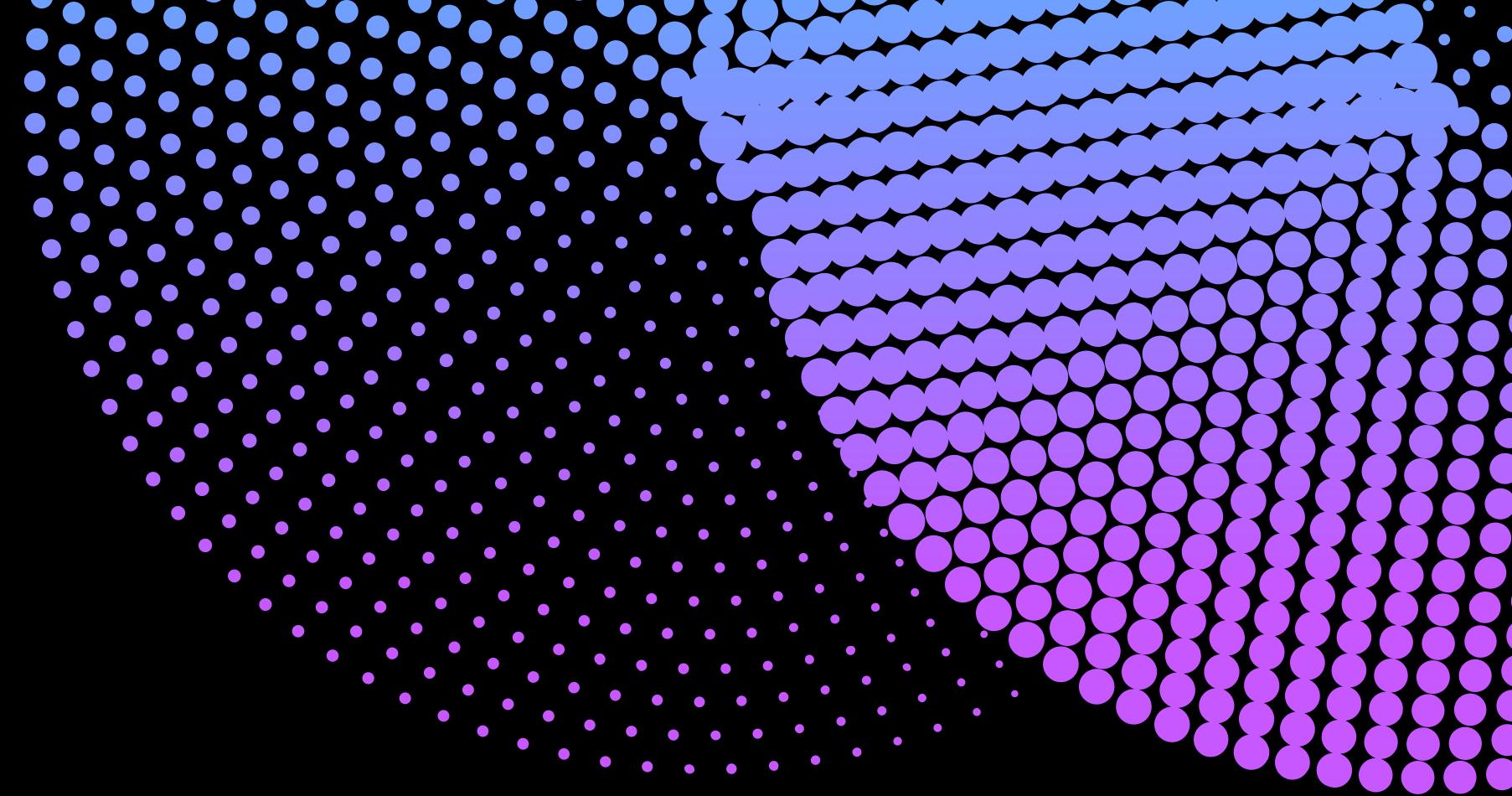
Nilai entropi rata-rata meningkat dari 4,689 pada Caesar Cipher menjadi 4,972 pada skema super enkripsi, yang menunjukkan peningkatan tingkat keacakan data sekitar 6%. Peningkatan nilai entropi ini mengindikasikan bahwa ciphertext menjadi lebih sulit dianalisis secara statistik oleh pihak yang tidak berwenang.

Selain peningkatan keamanan, kombinasi algoritma ini tetap efisien karena tidak menambah ukuran data hasil enkripsi, sehingga tidak memerlukan tambahan ruang penyimpanan maupun bandwidth.



5

Keterbatasan dan Peluang Penelitian Lanjutan



Meskipun kombinasi Caesar Cipher dan Vigenère Autokey terbukti mampu meningkatkan keamanan penyimpanan data teks, penelitian ini juga menemukan beberapa keterbatasan. Salah satu keterbatasan utama adalah dukungan karakter yang masih terbatas, umumnya hanya pada huruf kapital, sehingga penerapannya kurang optimal untuk data teks modern yang mengandung angka dan simbol.

Selain itu, penggunaan sistem kriptografi simetris menimbulkan tantangan dalam manajemen dan distribusi kunci, karena proses enkripsi dan dekripsi harus menggunakan kunci yang sama. Kelemahan ini dapat menjadi titik rawan apabila pengelolaan kunci tidak dilakukan dengan aman.

Oleh karena itu, penelitian lanjutan disarankan untuk mengembangkan dukungan set karakter penuh serta mengintegrasikan kombinasi algoritma ini dengan kriptografi asimetris dalam arsitektur hibrida guna meningkatkan keamanan dan fleksibilitas penerapan.

Terima
kasih

