

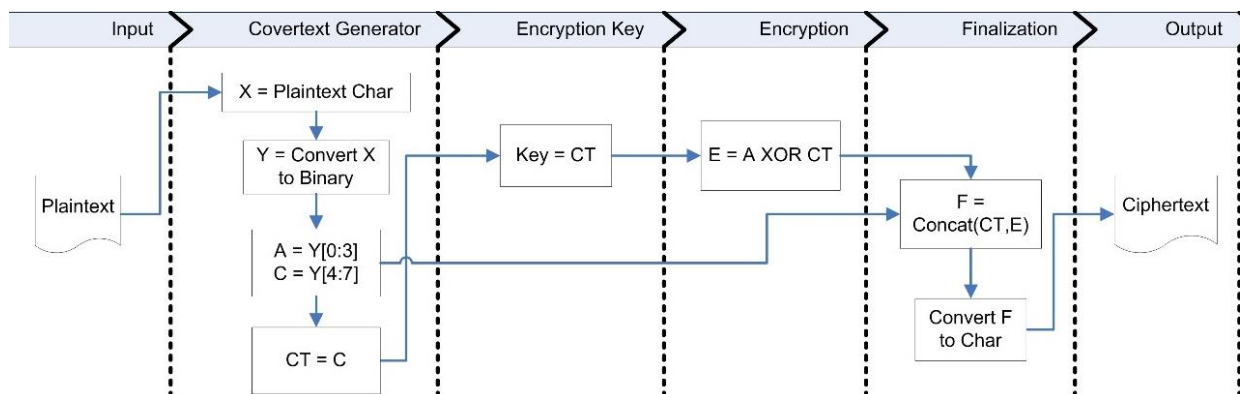
“Desain Model Enkripsi Light Parallel Encryption with Digit Arithmetic of Coverttext (Light PDAC)”

**PENCIPTA**

1. Dr. Eka Ardhianto, S.Kom., M.Cs
2. Drs. Widiyanto Tri Handoko, M.Kom
3. Hari Murti, S.Kom., M.Cs.
4. Rara Sriartati Redjeki, SE., M.Kom.

**A. DESKRIPSI:**

“Model Enkripsi Light Parallel Encryption with Digit Arithmetic of Coverttext (Light PDAC) merupakan bentuk pengembangan model enkripsi Parallel Encryption with Digit Arithmetic of Coverttext (PDAC). Model enkripsi ini menggabungkan teknik kriptografi dengan steganografi. Model enkripsi ini terbagi menjadi beberapa bagian yaitu: Coverttext Generator, Encryption Key Generator, Encryption, Finalization. Coverttext Generator berfungsi untuk membangkitkan coverttext. Coverttext adalah nilai dalam bentuk bit/byte yang digunakan sebagai “cover” dalam konteks steganografi. Encryption key generator berfungsi membangkitkan kunci enkripsi “key”. Kunci enkripsi digunakan sebagai sandi dalam proses enkripsi. Proses enkripsi menggunakan logika XOR menghasilkan encrypted text. Bagian finalization melakukan proses penggabungan coverttext dengan encrypted text menjadi ciphertext.”



Gambar. Desain Model Enkripsi Light PDAC.

Penjelasan:

Istilah	Keterangan
Plaintext	Bentuk informasi/data/pesan rahasia atau yang memiliki tingkat kerahasiaan atau yang memiliki akses terbatas
X	Setiap karakter dari plaintext
Y	Bentuk biner dari X
A	Nilai biner Y dengan urutan 0 sampai 3
C	Nilai biner Y dengan urutan 4 sampai 7
CT	Coverttext yang diambil dari nilai C
Key	Kunci enkripsi yang diambil dari nilai CT
E	Encrypted Text, sebagai hasil proses enkripsi antara A dengan CT menggunakan XOR
F	Hasil penggabungan E dengan CT
Ciphertext	Bentuk plaintext yang telah selesai di enkripsi

## B. HASIL PROSES

<b>Bentuk Output</b>	Bentuk output dari model enkripsi Light PDAC adalah ciphertext. Bentuk ciphertext ini adalah untaian karakter hasil enkripsi plaintext yang tidak memiliki arti/makna. Berikut adalah contohnya:	
	<b>Plaintext (input)</b>	<b>Ciphertext (output)</b>
	nice to see you that you are researching in the information security	icw#} f#vdd% nt%qofq\$qqq"arg"reqwar qnoha%ho% la(jgolxoc~kon"aecgtor
<b>Capaian lain</b>	Parameter lain yang dicapai Light PDAC adalah ukuran file ciphertext. Light PDAC memiliki ukuran yang sama pada file ciphertext dengan file plaintext.	

## C. IMPLEMENTASI

Model ini dapat diimplementasikan menggunakan bahasa pemrograman sesuai dengan kondisi aplikasi komputer/mobile yang akan dibangun.