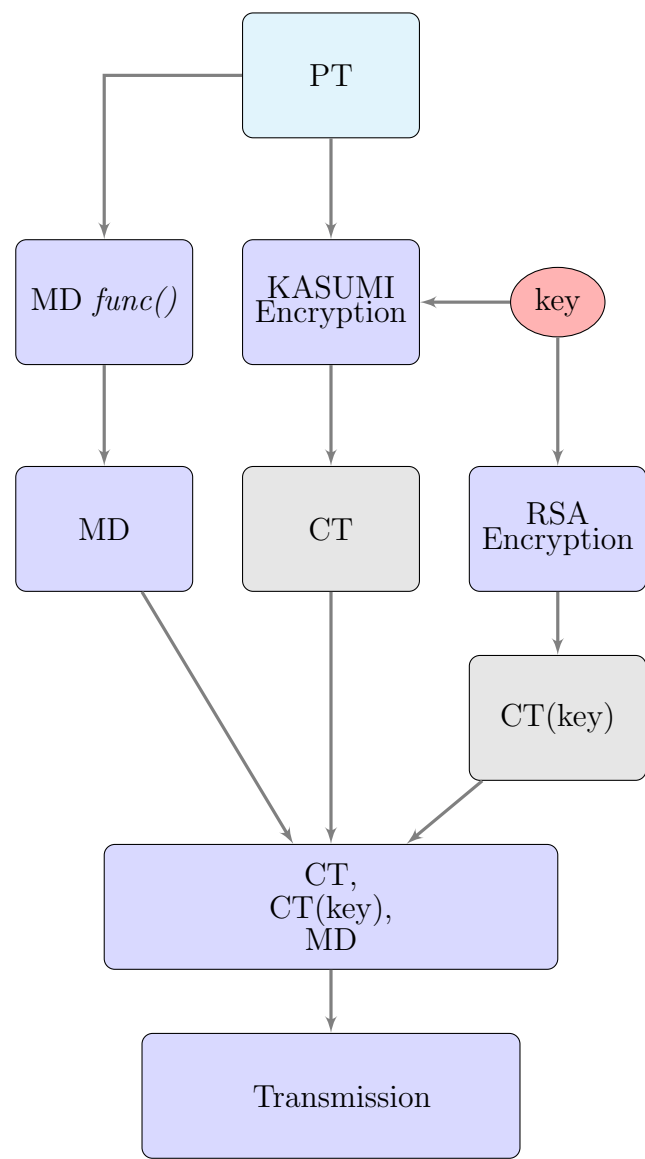# Proposed Hybrid Cryptosystem

November 13, 2022

Encryption Process

Decryption Process

```
                    ┌──────────────┐
                    │     CT,      │
              ┌─────┤   CT(key),   ├─────────────┐
              │     │      MD      │             │
              │     └──────┬───────┘             │
              │            │                     │
         ┌────▼───┐   ┌────▼────┐           ┌────▼───┐
         │   CT   │   │ CT(key) │           │   MD   │
         └────┬───┘   └────┬────┘           └────▲───┘
              │            │                     │
              │      ┌─────▼─────┐               │
              │      │    RSA    │               │         ┌──────────┐
              │      │ Decryption│          ┌────┤         │ Compare()│──match──▶ accept
              │      └─────┬─────┘          │    └──────────┘
              │            │                     │   not match
              │         ┌──▼──┐                  │        │
              └────┐    │ key │                  │        ▼
                   │    └─────┘                  │      reject
              ┌────▼───────┐  ┌─────┐  ┌────────┐  ┌────────┐
              │  KASUMI    │─▶│ PT  │─▶│MD func()│─▶│   MD   │
              │ Decryption │  └─────┘  └────────┘  └────────┘
              └────────────┘
```