`mango-rekey` - RSA Key Generation for Mango Publishers and UDMI site model

This Python script generates RSA key pairs for each publisher in a Mango JSON file, saves the keys in separate files within a structured directory following the UDMI site model data structure, and updates the JSON file with the new key values.

Usage

1. **Clone the repository:**

```
git clone [https://github.com/pisuke/mango-rekey]
(https://github.com/pisuke/mango-rekey)
```

2. **Install dependencies:**

```
pip install -r requirements.txt
```

3. **Run the script:**

```
python mango-rekey.py -i input.json -o output.json
```

Replace input.json and output.json with the paths to your input and output JSON files, respectively.

Input:

The iput is a Mango JSON file containing a publishers array, where each publisher is represented by a JSON dictionary.

Output:

The output Mango JSON file where the rsaPrivateKey and rsaPublicKey fields are updated for each publisher.

The private and public keys for each publisher are also saved in separate PEM files within a directory named after the publisher's name in a folder named `devices`, following the UDMI site model file structure.

Key Points:

No Passphrase: The generated private keys are not encrypted in this example. For increased security, encrypt private keys with a strong passphrase.

Output File:

The script modifies the input JSON file by default. Use the -o option to specify a different output file if you want to preserve the original.

Requirements:

- Python 3.6 or later
- The `cryptography` library
- The `absl-py` library