

ক্রিপ্টোগ্রাফি কি?

আমরা এই অধ্যায়ে যে বিষয়গুলো নিয়ে আলোচনা করবো-

- ক্রিপ্টোগ্রাফি কি?
- কি কি ধরনের ক্রিপ্টোগ্রাফি রয়েছে?
- ক্রিপ্টোগ্রাফি টুলসসমূহ
- ক্রিপ্টোএনালাইসিস কি?
- কিভাবে ক্রিপ্টোএনালাইসিস করা হয়?
- ক্রিপ্টোএনালাইসিস টুলসসমূহ

ক্রিপ্টোগ্রাফি কি?

cryptography হচ্ছে "সাংকেতিক উপায়ে তথ্য আদান বা প্রদানের ব্যবস্থা"।
এক জায়গা থেকে অন্য জায়গায় তথ্য পাঠানোর জন্য ক্রিপ্টোগ্রাফি ব্যবহার করা হয়, যাতে আন-অথোরাইজড কেউ সেটা বুঝতে না পারে।

কি কি ধরনের ক্রিপ্টোগ্রাফি রয়েছে?

সাধারণত দুই ধরনের ক্রিপ্টোগ্রাফি রয়েছে।

১) সিমেন্টিক এনক্রিপশন

২) এসিম্যাটিক এনক্রিপশন

সিমেট্রিক এনক্রিপশন

যখন এনক্রিপশন এবং ডিক্রিপশন এর জন্য সেইম কী ব্যবহার করা হয় তখন থাকে সিমেট্রিক এনক্রিপশন বলে।



এসিম্যাটিক এনক্রিপশন


যখন এনক্রিপশন এবং ডিক্রিপশন এর জন্য ভিন্ন কী ব্যবহার করা হয় তখন থাকে এসিম্যাটিক এনক্রিপশন বলে।

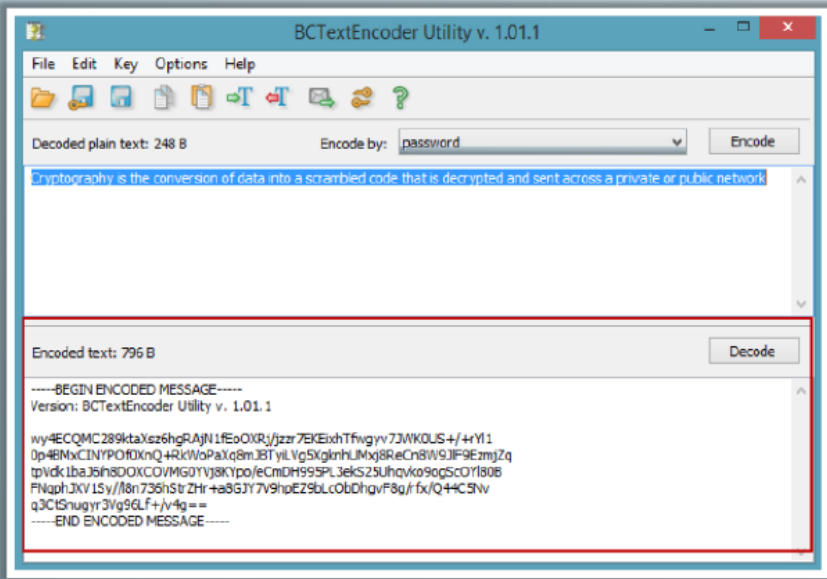


ক্রিপ্টোগ্রাফি টুলসসমূহ

ক্রিপ্টোগ্রাফি করার জন্য বিভিন্ন ধরনের টুল পাওয়া যায়। যেমন একটি টুল হলো- BCTestEncoder


Cryptography Tool: **BCTestEncoder**





The screenshot shows the BCTestEncoder Utility v. 1.01.1 interface. It has a menu bar (File, Edit, Key, Options, Help) and a toolbar. The 'Decoded plain text' field shows 248 B. The 'Encode by' dropdown is set to 'password'. The 'Encoded text' field shows 796 B. The encoded message is displayed in a text area, starting with '-----BEGIN ENCODED MESSAGE-----' and ending with '-----END ENCODED MESSAGE-----'. The version is BCTestEncoder Utility v. 1.01.1.

- BCTestEncoder encrypts **confidential text** in your **message**
- It uses strong and approved symmetric and public key algorithms for **data encryption**
- It uses public key encryption methods as well as **password-based encryption**



<http://www.jetico.com>

ক্রিপ্টোনালাইসিস কি?

ক্রিপ্টোনালাইসিস হল সিক্যুরড কম্যুনিকেশন অ্যানালাইজ করে ব্রেক করে ফেলার বিজ্ঞান!

কিভাবে ক্রিপ্টোনালাইসিস করা হয়?

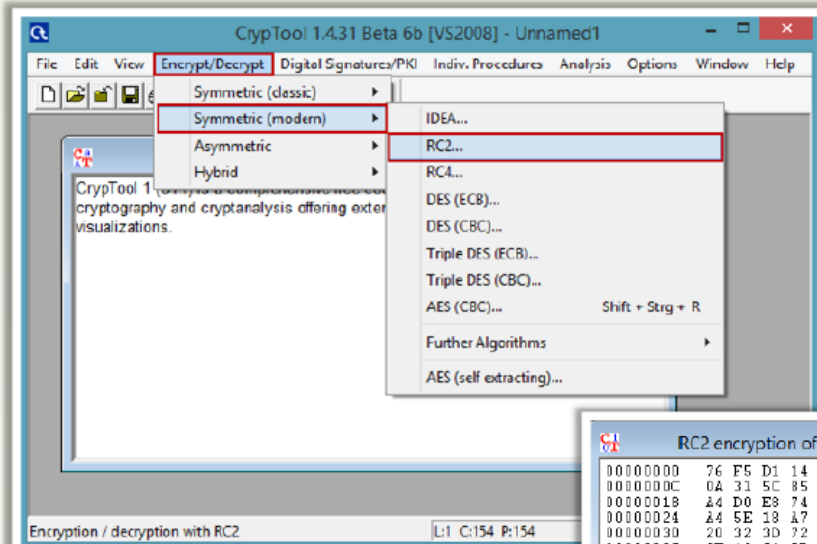
- ব্রুট ফোর্স এটাক এর মাধ্যমে বিভিন্ন কী জেনারেট করে ট্রাই করা হয়
- সোশ্যাল ইঞ্জিনিয়ারিং করে কী জানার চেষ্টা করা হয়।
- অটোমেটিক পাসওয়ার্ড জেনারেটর টুল দিয়ে ট্রাই করা যেতে পারে।

ক্রিপ্টোনালাইসিস টুলসসমূহ

ক্রিপ্টোনালাইসিস টুলস ব্যবহার করে ম্যাসেজ কালেক্ট করা যেতে পারে।

ক্রিপ্টোনালাইসিস এর অনেকগুলো টুল রয়েছে। যেমন-CrypTool

Cryptanalysis Tool: **CrypTool**



<http://www.cryptool.org>



■ CrypTool is a free e-learning program in the area of **cryptography** and **cryptanalysis**

■ Subprojects of CrypTool:

- CrypTool 1 (CT1)
- CrypTool 2 (CT2)
- JCryptTool (JCT)
- CrypTool-Online (CTO)

