Ludwig-Maximilans-
Universität München
Dr. Pascal Reisert

Wintersemester 2018/2019
9. Januar 2019

Übungen zur Kryptographie
Lösungsskizze

Preisaufgabe

Der Klartext lautet:

"It has been witnessed in history that every advance of encryption has been defeated by advances in hacking. In particular, with the advent of Shor's factoring algorithm, most of the currently used cryptographic infrastructure will be defeated by quantum computers. On the contrary, quantum key distribution (QKD) offers unconditional security ensured by the law of physics. QKD uses the fundamental unit of light, single photons, encoded in quantum superposition states which are sent to a distant location. By proper encoding and decoding, two distant parties share strings of random bits called secret keys. However, due to photon loss in the channel, the secure QKD distance by direct transmission of the single photons in optical fibers or terrestrial free space was hitherto limited to a few hundred kilometers. Unlike classical bits, the quantum signal in the QKD cannot be noiselessly amplified owing to the quantum no-cloning theorem. The main challenge for a practical QKD is to extend the communication range to long distances, ultimately on a global scale. A promising solution to this problem is exploiting satellite and space-based links. That way, one can conveniently connect two remote points on Earth with greatly reduced channel loss because most of the photons' propagation path is in empty space with negligible loss and decoherence."

Der Schluessel ist:

```
D33467BD7BB837D35D01CA181F88CD5F3ECA1DF40DD7107E2CFA6128D9457F40E3FB52BF69
E8909E75C2452855F892D64833C5E1A9142CD5CD241DFA2E0C8F9136612CC582112D4F32C4B
E2B4085A8390A160A7C046E0DB981F7359D6AB30786D50BF823BBE3ADC95A8C02A581425DFC
F56E2ED8A15CE25C6E8B1349838CB59145EC45CBDCA4E8661A2B46AE1EA6C1829646921A9F0
FEE03F13862544AE506D8504C4648026A6F7424D1A7C5365E75CA5F76E9154A7E4032993848
0C34C8F0B12B9C1985A2D34FECCA138D93BF0FED0174EB6E5FAC1E4FD1133613F81B9A6EA76
1A0BC251A73A27DE5F03153B28E7ABA567A11A08A1D01AF74E7A609F39EA16CBB465A960E44
672EB8E53D217644FDFD86B1F7C23D917C8C8C3B0DF66113AB0B2C1156E79C030631DE306A6
62566367EAD012B2D654C9019624C4322578AA5367C4E6083B8F095C15D65B3D3EF87511548
D066C10D1C68C5D553AF9E6EDD943E903468A2281B0ACA9FD1FBE87A094CA61644F69FB5FC8
9DF3B98826ADD52D3EC718EDAFDC4326AB101981745899F3A01C30EC3D5D76CF8A5037384B2
5A277DBD4F0FEF839D1FFED186268522E71231B75B58F256F5BB8A2664961E89A1FF4292BD2
F4A0592B55C5EE3B8B5A8508413D91B96781432D9D13F44F114B935479203B1777AA1D90D62
4A9593F3382113C77BCE8D05AE4290FF0C7C764F9543612D558C0414071EA4065B4C74BC33D
CE9405FA69A829B79601428CD12167885A12CA3B74288685F7C92D5544F2F
```

Die Periode ergibt sich z.B. indem man immer größere Abschnitte mit $\oplus$ addiert. Hat man die richtige Periodenlänge erreicht, so kürzt sich das OTP heraus. Dies erkennt man dadurch, dass dann ein Text entsteht, der dem $\oplus$ zweier natürlicher Texte in englischer Sprache entspricht. Dies kann man z.B. überprüfen indem man auf ein verschwindendes 8tes Bit testet oder den Koinzidenzindex ansieht.

Anschließend kann man mit häufigen Bi-, Tri-, Multigrammen erste Wörter herausfinden und ggf. manuell ergänzen. Je größer dieses "Wörterbuch" ist auf das man überprüft, desto mehr Wörter des Klartextes wird man finden. Es bleibt jedoch zumeist ein Restanteil an verschlüsseltem Text, den man dann aber leicht erraten kann. In diesem Fall genügt es jedoch einen genügend langen Text (z.B. eine geeignete Kombination von 3 oder 4 Wörtern) zu finden und mittels einer kurzen Onlinesuche dem gesuchten Abschnitt des Artikels "Satellite-relayed intercontinental quantum network" zuzuordnen.