O sekrecie pośród wielu, Ali Babie i portfelu

1. **Wstęp**
   O czym będziemy mówić
   a) Przedstawienie (pytać, przerywać)
   b) Wprowadzenie do historyjki
2. **Szyfrowanie**
   Prywatne rozmowy Alicji i Boba
   a) Szyfr Cezara
   b) Szyfr podstawieniowy
   c) Szyfr XOR
   d) Szyfr Vigenère'a
   e) RSA
3. **Orzeł i reszka na odległość**
   Kłótnia Alicji i Boba
   a) Zobowiązanie bitowe
      - Idealna skrzyneczka na kluczyk
      - Zamknięcie skrzynki i wysłanie
      - Wysłanie klucza
   b) Rozwiązanie z *commitment scheme*
   c) Inne:
      - Papier, kamień, nożyce
      - Gra w karty (dwa kluczyki)
4. **Dowód z wiedzą zerową**
   Przekonanie o rozwiązaniu zagadki manuskryptu
   a) Przekonanie prezentera
      - Prawdopodobieństwo $\mathbb{P}[X] = \frac{1}{2^{40}}$
   b) Fałszerstwo Boba
      - Wartość oczekiwana $\mathbb{E}[X] = 80$.
   c) Właściwości
      - Prezenter przekonany
      - Fałszerz nikogo nie przekona
      - Zero wycieku danych
      - Nierozróżnialność
   d) Inne:
      - Układanie kostki rubika
      - Logowanie w systemie internetowym
5. **Podział sekretu**
   Zabezpieczenie hasła pośród znajomych
   a) Podział na n kluczy, tylko wszystkie otwierają
      - Zwykłe dodawanie
      - Dodawanie modulo
      - Xorowanie
   b) Podział na n kluczy, każde k otwiera
      - Poprzedni pomysł $\binom{n}{k}$ razy
      - Interpolacja wielomianowa Lagrange'a
        – Twierdzenie
        – Konstrukcja
        – Dlaczego działa?
      - *Interpolacja Newtona, regresja
   c) Klucze ważone
6. **Podsumowanie**
   a) Przydatność matematyki w prawdziwym życiu (poruszone problemy)
   b) Inne problemy
      - Kto jest bogatszy?
      - Hashowanie
      - Szyfrowanie, łamanie szyfrów
   c) Zachęta do:
      - OI(G), OM(G)
      - Fundusz
      - MOKIK
      - Poszukiwania ciekawych tematów
      - Własnej pracy
        (`http://informatyka.wroc.pl/security`)
        (`http://cubix.one.pl/files/szyfry.zip`)
      - Kontaktu: mail, WWW, FB
   d) Podziękowanie
7. * **RSA** *Przydatne: kongruencje, MTF, Chińskie tw. o resztach,* *Tw. Eulera, Ciało* $\mathbb{Z}_p$
   a) Zasada działania
   b) Generowanie kluczy
      - Znajdź 2 duże liczby pierwsze p, q podobnej wielkości, ale o dużej różnicy
      - Niech $n := pq$, oblicz $\varphi(n) = (p-1)(q-1)$
      - Weź losowe e t.ż. $\mathbb{NWD}(e, \varphi(n)) = 1$
      - Znajdź d t.ż. $ed \equiv 1 \pmod{\varphi(n)}$
      - Klucz publiczny: (n, e)
      - Klucz prywatny: (n, d)
   c) Szyfrowanie: $m^e \mod n$
   d) Deszyfrowanie: $m^d \mod n$
   e) Dlaczego...
      - ...działa (de)szyfrowanie?
      - ...trudno złamać?
   f) Zastosowanie do zobowiązania bitowego
   g) **2 kluczyki w grze w karty na odległość