QUANTUM CRYPTOGRAPHY

- CAN BE MADE UNBREAKABLE
- CANNOT BE INTERCEPTED CORRECTLY
- ANY INTERCEPTION CAN BE DETECTED
- UNIQUE SYSTEM OF KEY MANAGEMENT (NON RSA, DIFFIE-HELLMAN)

POLARISED TRANSMISSION

RECTILINEAR

1 1 0 1 0

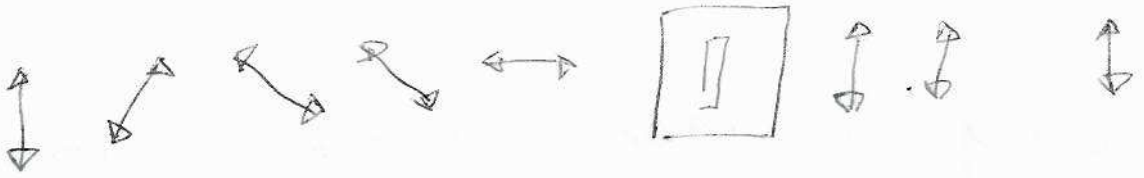
1 1 0 1 0

DIAGONAL

1 1 0 1 0

1 1 0 1 0

MIXED POLARISATIONS



Diagonal polarisations pass through vertical filter with probability of 50%.

ONE TIME PAD CODING SCHEME

TRANSMISSION	↕	↗	↖	↘	↔
CODING SCHEME (ONE TIME PAD)	+	×	×	×	+
DATA	1	1	0	0	0

PROBLEM OF INTERCEPTION

- WITHOUT KNOWLEDGE OF SCHEME INTERCEPTOR WILL NOT HAVE CORRECT (+, ×) FILTER
- USE OF INCORRECT FILTER WILL RESULT IN ERRORS WITH PROBABILITY OF 50 %

DETECTION OF INTERCEPTION

- USE AGREED TEST SEQUENCE WITH CODING SCHEME
- INTERCEPTOR WILL CORRUPT DATA

KEY MANAGEMENT

- CANNOT USE PHYSICAL TRANSPORT, RSA or DIFFIE - HELLMAN FOR ONE TIME PAD (CONVENTIONAL METHODS ASSUMED TO BE BREAKABLE)
- A SENDS B LONG TRANSMISSION WITH SECRET CODING SCHEME
- B GUESSES SCHEME RANDOMLY AND THEREFORE RECEIVES CORRUPTED DATA.
- A GIVES B SCHEME (BUT NOT DATA) IN CLEAR
- B RESPONDS WITH INFORMATION ON CORRECT 'GUESSES' (OF SCHEME ONLY)
- A & B NOW SHARE CORRECT SUBSET OF ORIGINAL CODING SCHEME

INTERCEPTION OF KEY MANAGEMENT

- INTERCEPTOR C WILL MAKE DIFFERENT 'GUESSES' COMPARED WITH B
- IF B GUESSED CORRECTY AND C INCORRECTLY, C HAS NO INFORMATION
- A and B MAY GUARD AGAINST DATA CORRUPTION THROUGH INTERCEPTION BY USING SUBSET OF AGREED DATA AS TEST SEQUENCE

The info that B gives A is noise because C uses diff strategy.