




























<p>A slide deck entirely in Comic Sans.</p> 	<p>Ctrl+F'ing to see how many times I'm cited and finding "0 results".</p> 	<p>"Working" remotely.</p> 
<p>16-bit AES.</p> 	<p>17 slides for a 3-minute rump session talk.</p> 	<p>2 to 4 kilograms of top quality amphetamines.</p> 
<p>2-sentence Eurocrypt reviews.</p> 	<p>4mm reasonable margins.</p> 	<p>A 25-year old policy on sexual harassment.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>A career-limiting card game.</p> 	<p>A dancing cryptographer.</p> 	<p>A genuine attempt to configure IPsec.</p> 
<p>A hand wavy argument.</p> 	<p>A non-fabricated use of pairings.</p> 	<p>A painfully slow Tor masturbation session.</p> 
<p>A popup Skype notification from “lovemachine69” during my keynote talk.</p> 	<p>A proof that appears in the “full version”.</p> 	<p>A shepherd that won’t budge.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Aaron Aaronson's insistence on alphabetical author ordering.</p> 	<p>Accidentally sexting my co-supervisor.</p> 	<p>Actually being "sorry for the late reply".</p> 
<p>Actually efficient indistinguishability obfuscation.</p> 	<p>Adleman-Rivest-Shamir encryption (the ARSE algorithm).</p> 	<p>An "anonymous" reviewer insisting I cite 6 papers by the same author.</p> 
<p>An IACR board meeting.</p> 	<p>An insecure VPN straight to the Kremlin.</p> 	<p>An overfull hbox.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>An SSL vulnerability with a silly name.</p> 	<p>Arriving 13 minutes late to a 15 minute talk and having the gall to ask a question.</p> 	<p>Beefing up my Proposition to a Theorem because I'm that awesome.</p> 
<p>Best rejected paper award.</p> 	<p>Brexit.</p> 	<p>Checking my Google Scholar profile daily.</p> 
<p>Chocolate-covered shrimp.</p> 	<p>Citing personal communication.</p> 	<p>Crippling student debt.</p> 










Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Crypto wars.</p> 	<p>Deliberately hiding inefficiencies inside the big O.</p> 	<p>Deliberately not referencing a superior paper.</p> 
<p>Diffie but definitely not Hellman.</p> 	<p>Double ROT-13.</p> 	<p>Drinking alone.</p> 
<p>Dropping the word Blockchain into my research proposal as many times as possible.</p> 	<p>Encrypted database security definitions.</p> 	<p>Explaining what my job is at a family reunion.</p> 

Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Fighting over LaTeX syntax.</p> 	<p>Filing a patent application for modular multiplication... in 2017.</p> 	<p>Forgetting my VGA adapter.</p> 
<p>Frantically taking notes during every talk.</p> 	<p>Getting a fourth cookie during a coffee break because I have no one to talk to.</p> 	<p>Getting rejected, but then taking immediate solace in the fact that the selection of papers was a difficult and challenging task.</p> 
<p>Getting stuck at the French-speaking banquet table.</p> 	<p>Getting tenure, then chilling the f— right out!</p> 	<p>Getting turned on by a proof.</p> 

Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Going straight to journal.</p> 	<p>Having to write a polite rebuttal to the reviewer who clearly didn't read past page 2.</p> 	<p>Hillary Clinton's BlackBerry.</p> 
<p>Home-baked, snake oil crypto.</p> 	<p>HTTPS everywhere!</p> 	<p>Ignoring reviewer comments and resubmitting immediately.</p> 
<p>Ignoring the session chair flashing 5 minutes left because I've got 23 slides to go.</p> 	<p>Including an XKCD comic in my slides because I'm so original.</p> 	<p>Knapsack cryptosystems, revisited.</p> 

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**










**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

<p>LNCS' 25-foot margins.</p> 	<p>Making claims in the submission that you hope you can achieve before the rebuttal.</p> 	<p>Maths-terbation.</p> 
<p>My <i>h</i>-index.</p> 	<p>My butt.</p> 	<p>My genitals.</p> 
<p>My inappropriate supervisor.</p> 	<p>My relationship status.</p> 	<p>My sex life.</p> 

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**










**Cards
Against
Cryptography**

**Cards
Against
Cryptography**










**Cards
Against
Cryptography**

**Cards
Against
Cryptography**










**Cards
Against
Cryptography**

<p>My side job as an incompetent security consultant.</p> 	<p>My Silk Road purchase history.</p> 	<p>My supervisor's morning breath.</p> 
<p>Nigel Smart's new Hawaiian shirt.</p> 	<p>Overselling it hard in the introduction.</p> 	<p>Password1.</p> 
<p>Picturing the FSE audience naked.</p> 	<p>Politely starting an answer with "That's a good question...", when the question is actually idiotic.</p> 	<p>Post-quantum RSA.</p> 

Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Preparing for two weeks to give a 15-minute presentation to a room of 7 people all on their laptops.</p> 	<p>Pretending to understand.</p> 	<p>Publishing anyway.</p> 
<p>Putting an outdoors-y photo on my academic webpage to look well-rounded.</p> 	<p>Quadruple XOR.</p> 	<p>Quickly trying to peek at someone's badge as I shake their hand, but it's flipped backwards.</p> 
<p>Reading the person in front's emails.</p> 	<p>Relatives who ask me to help them install their printer on Windows.</p> 	<p>Rogaway's loose morals.</p> 

Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Satoshi Nakamoto.</p> 	<p>Sending an email at 11pm so people think I work hard.</p> 	<p>Sexual tension.</p> 
<p>Skype dropping out every 10 to 15 seconds.</p> 	<p>Spending 3 Bitcoin on pizza in 2012.</p> 	<p>Spending all of my Levchin prize money on cocaine.</p> 
<p>Springer's editorial team.</p> 	<p>Starting a conversation with "When did you fly in?", because I have nothing interesting to say.</p> 	<p>Taking a group shower with my recent co-authors.</p> 

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**

**Cards
Against
Cryptography**










**Cards
Against
Cryptography**

**Cards
Against
Cryptography**










**Cards
Against
Cryptography**

**Cards
Against
Cryptography**










**Cards
Against
Cryptography**

<p>Telling anyone who'll listen quite how busy I am.</p> 	<p>Thanking the anonymous reviewers for their "useful" comments.</p> 	<p>The awkward question the chair asks when nobody understood the talk.</p> 
<p>The awkward silence of 8 people standing in a circle during the afternoon coffee break.</p> 	<p>The great firewall of China.</p> 	<p>The great paywall of IEEE.</p> 
<p>The intoxicating aroma of 12 PhD students in one office.</p> 	<p>The North Korean Cryptographic Standard.</p> 	<p>The NSA's massive stack of amateur porn.</p> 

Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>The one really hot person at CHES registration drinks.</p> 	<p>The one suit I own for meetings with industry.</p> 	<p>The person in the front row taking photos of every slide.</p> 
<p>The secret flash drive hidden in my underwear.</p> 	<p>The walking zombie corpse of Claude Shannon.</p> 	<p>Thinking I'm so clever for using pictures of Alice (Cooper) and Bob (Marley).</p> 
<p>Trying to make TCC friends at the bar in order to get the IACR 7-conference grand slam.</p> 	<p>Turbulent bowel movements in the middle of my Asiacrypt presentation.</p> 	<p>Turning up to one meeting and claiming co-authorship.</p> 

Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography

<p>Unbreakable military-grade encryption.</p> 	<p>Undergrads.</p> 	<p>Using “it clearly follows” when the implied following is anything but clear.</p> 
<p>Using Beamer because it’s social suicide to use PowerPoint.</p> 	<p>Using indecipherable, non-standard notation to hide a dodgy proof.</p> 	<p>Vital sugar beet auctions.</p> 
<p>Wearing a conference t-shirt... in public.</p> 	<p>Wistfully looking out of the window of my overly-cramped PhD office.</p> 	<p>Writing a reference for someone I can’t remember meeting.</p> 

Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography
Cards Against Cryptography	Cards Against Cryptography	Cards Against Cryptography